Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date October 13, 2020

Original Release Date July 9, 2020

Superseding Document

Status	Final
Series/Number	NIST Interagency or Internal Report 8286
Title	Integrating Cybersecurity and Enterprise Risk Management (ERM)
Publication Date	October 2020
DOI	https://doi.org/10.6028/NIST.IR.8286
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8286/final
Additional Information	

National Institute of Standards and Technology
U.S. Department of Commerce

Draft (2nd) NISTIR 8286

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine
Stephen Quinn
Greg Witte
R. K. Gardner

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286-draft2

National Institute of Standards and Technology
U.S. Department of Commerce

Draft (2nd) NISTIR 8286

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine
Applied Cybersecurity Division
Information Technology Laboratory

Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

Stephen Quinn
Computer Security Division
Information Technology Laboratory

R. K. Gardner
New World Technology Partners
Annapolis, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286-draft2

July 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8286
76 pages (July 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286-draft2

Public comment period: *July 9, 2020* through *August 21, 2020*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8286@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The increasing frequency, creativity, and severity of cybersecurity attacks means that all enterprises should ensure that cybersecurity risk is receiving appropriate attention within their enterprise risk management (ERM) programs. This document is intended to help individual organizations within an enterprise improve their cybersecurity risk information, which they provide as inputs to their enterprise's ERM processes through communications and risk information sharing. By doing so, enterprises and their component organizations can better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives. Focusing on the use of risk registers to set out cybersecurity risk, this document explains the value of rolling up measures of risk usually addressed at lower system and organization levels to the broader enterprise level.

Keywords

cybersecurity risk management; cybersecurity risk measurement; cybersecurity risk profile; cybersecurity risk register; enterprise risk management (ERM); enterprise risk profile.

Acknowledgments

The authors wish to thank all individuals, organizations, and enterprises that contributed to the creation of this document. This includes Donna Dodson, Mat Heyman, Nahla Ivy, Naomi Lefkovitz, Rodney Petersen, Vicky Pillitteri, Ron Ross, and Adam Sedgewick of NIST; Larry Feldman, Heather Mills, and Dan Topper of Huntington Ingalls Industries (HII); and Karen Scarfone of Scarfone Cybersecurity. Organizations and individuals who provided feedback on the first public comment draft include Aon, Association of Local Government Auditors, Booz Allen Hamilton, Cyber-ERM Community of Interest, Cybersecurity and Infrastructure Security Agency (CISA), FAIR Institute, Forescout Technologies, Internet Security Alliance, Mosaic 451, Navigation Advisors, Nuclear Regulatory Commission (NRC), Profitabil-IT, RiskLens, RSA, Threat Sketch, US Air Force, US Department of Education, US Department of Energy, US Navy, Simon Burson, John Kimmins, Norman Marks, Paul Rohmeyer, Ellen Swanson, and Douglas Webster.

Audience

The primary audience for this publication include cybersecurity professionals at all levels who understand cybersecurity but may be unfamiliar with the details of enterprise risk management (ERM).

The secondary audience includes corporate officers, high-level executives, ERM officers and staff members, and others who understand ERM but may be unfamiliar with the details of cybersecurity.

All readers are expected to gain an improved understanding of how cybersecurity risk management and ERM complement and relate to each other and the benefits of integrating their use.

Trademark Information

Document Conventions

The term ‘step’ or ‘steps’ is used in multiple frameworks and documents. If the term ‘step’ is referring to anything other than the meaning from the ERM Playbook from Figure 2, it will be preceded by a document or framework to differentiate its context (e.g., ‘NIST Cybersecurity Framework Step 1: *Prioritize and Scope*’.)

Note to Reviewers

This is the flagship document in a series focused on integrating cybersecurity and Enterprise Risk Management (ERM) practices. Subsequent documents will explain and provide actionable guidance on topics introduced in this document.

This draft is provided to promote greater understanding of the relationship between cybersecurity risk management and ERM as well as the benefits of integrating these approaches. NIST welcomes comments on any aspects of this draft and requests that reviewers especially consider the following questions.

Does this draft adequately and appropriately:

- define and differentiate the relationship between cybersecurity risk management and ERM?
- define and distinguish between systems, organizations, and enterprises?
- explain the value of integrating cybersecurity risk management and ERM?
- provide information in a manner that is comprehensible to the cybersecurity and enterprise risk managers who are intended to benefit from the publication?
- illustrate ways in which organizations and enterprises may integrate cybersecurity risk management and ERM?
- describe pertinent roles?
- articulate the importance of risk consequences to capital (balance sheet content), and not just costs or net earnings, as a highly significant enterprise risk issue?
- show that cybersecurity risk measures must aggregate and roll up to the same few core measures that all other enterprise risks use in order to compare them on the same footing and to allocate risk resources (e.g., expenditures, capital, cash) across all risk categories?

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: nistir8286@nist.gov

Executive Summary

Office of Management and Budget (OMB) Circular A-11 defines risk as "the effect of uncertainty on objectives" [1]. The effect of uncertainty on *enterprise* mission and objectives may then be considered an "enterprise risk" that must be similarly managed. An *enterprise* is an organization that exists at the top level of a hierarchy with unique risk management responsibilities. Managing risks at that level is known as enterprise risk management (ERM) and calls for understanding the core risks that an enterprise faces, determining how best to address those risks, and ensuring that the necessary actions are taken. In the Federal Government, ERM is considered to be "an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos" [1].

Cybersecurity risk is an important type of risk for any enterprise. Others include but are not limited to financial, legal, legislative, operational, privacy, reputational, safety, strategic, and supply chain risks [2]. As part of an ERM program, corporate officers and board members at the highest levels of governance and direction for the enterprise who have fiduciary and reporting responsibilities not performed anywhere else in the enterprise are expected to holistically manage the combined set of risks.

The individual organizations that comprise every enterprise are experiencing an increase in the frequency, creativity, and severity of cybersecurity attacks. All organizations and enterprises, regardless of size or type, should ensure that cybersecurity risk receives appropriate attention as they carry out their ERM functions.

Since enterprises are at various degrees of maturity regarding the implementation of risk management, this document offers NIST's cybersecurity risk management expertise to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise's ERM programs.

Many resources—such as well-known frameworks from the Committee of Sponsoring Organizations (COSO), Office of Management and Budget (OMB) circulars, and the International Organization for Standardization (ISO)—document ERM frameworks and processes. They generally include similar approaches: identify context, identify risks, analyze risk, estimate risk importance, determine and execute the risk response, and identify and respond to changes over time. A critical risk document used to track and communicate risk information for all of these steps throughout the enterprise is called a *risk register* [1].[1] The risk register provides a formal communication vehicle for sharing and collaborating cybersecurity risk activities as an input to ERM decision makers. For example, *cybersecurity risk registers* are key aspects of managing and communicating about those particular risks.

At higher levels in the enterprise structure, those cybersecurity and other risk registers are ideally aggregated, normalized, and prioritized into *risk profiles*. A risk profile is defined by OMB

[1] OMB Circular A-11 defines a risk register as "a repository of risk information including the data understood about risks over time" [1].

Circular A-123 as "a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks" [3]. While it is critical that enterprises address potential negative impacts on mission and objectives, it is equally critical (and required for federal agencies) that enterprises plan for success. OMB states in Circular A-123 that "the [Enterprise Risk] profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)." Enterprise-level decision makers use the risk profile to choose which enterprise risks to address and to allocate resources and delegate responsibilities to appropriate risk owners. ERM programs should define terminology, formats, criteria, and other guidance for risk inputs from lower levels of the enterprise.

Cybersecurity risk inputs to ERM programs should be documented and tracked in written cybersecurity risk registers that comply with the ERM program guidance. However, most enterprises do not communicate their cybersecurity risk in consistent, repeatable ways. Methods such as quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are largely ad hoc and are sometimes not performed with the same rigor as methods for quantifying other types of risk within the enterprise.

In addition to widely using cybersecurity risk registers, improving the risk measurement and analysis methods used in cybersecurity risk management would boost the quality of the risk information provided to ERM. In turn, this practice would promote better management of cybersecurity at the enterprise level and support the enterprise's objectives.

There are readily available options for accomplishing each of these actions. Following these steps will help cybersecurity professionals understand what executives and corporate officers need to carry out ERM. They will also help high-level executives and corporate officers understand the challenges that cybersecurity professionals face when providing them with the information they are accustomed to getting for other types of risk.

Table of Contents

List of Appendices

List of Figures

322 **List of Tables**

332

1 Introduction

The terms *organization* and *enterprise* are often used interchangeably.[2] However, for the purposes of this document, an *organization* is defined as an entity of any size, complexity, or positioning within a larger organizational structure (e.g., a federal agency or company) [5]. An *enterprise* is an organization by this definition, but it exists at the top level of the hierarchy and has unique risk management responsibilities. In terms of cybersecurity risk management, most responsibilities tend to be carried out by individual organizations within an enterprise. The responsibility for tracking key enterprise risks and their impacts on objectives is held by corporate officers and board members who have fiduciary and reporting responsibilities not performed anywhere else in the enterprise.

Figure 1 depicts a notional enterprise with subordinate organizations, illustrating that one of those subordinate units has its own enterprise considerations. Both government and industry are represented in this depiction. Consider the example of the Department of Commerce as a higher-level enterprise with bureaus (e.g., Census Bureau, National Oceanic and Atmospheric Administration [NOAA], NIST) as lower-level enterprises and subordinate entities (e.g., NOAA's National Weather Service, NIST laboratories) representing organizations. In industry, consider mergers and acquisitions where an enterprise acquires another company, which itself was an enterprise, and then subordinates it within the higher-level enterprise's conglomeration of organizations and systems.[3] Each is supported by various *systems*, defined as "a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" [5].

[2] For example, NIST IR 8170 [4] uses *enterprise risk management* and *organization-wide risk management* interchangeably. The scope of IR 8170 includes smaller enterprises than this publication does, so an *enterprise* as defined in IR 8170 may be comprised of a single organization. The enterprises being discussed in this publication have more complex compositions.

[3] An enterprise can be thought of structurally as a portfolio (or set of portfolios). Just as a portfolio can be a combination of programs, projects, and lower-level portfolios, so too can an enterprise be comprised of one or more systems, organizations, and subordinate enterprises.

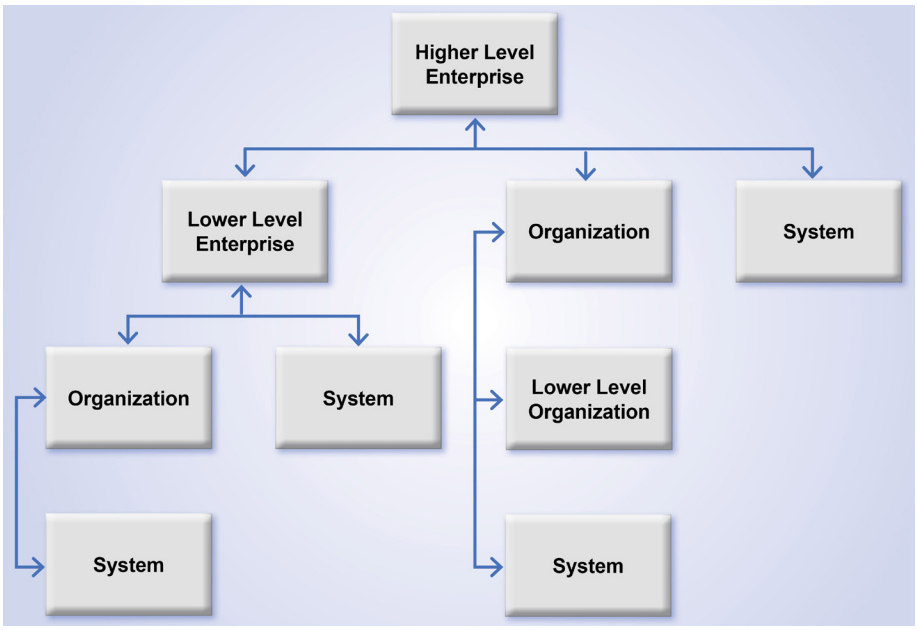


Figure 1: Enterprise Hierarchy for Cybersecurity Risk Management

1.1 Purpose and Scope

The purpose of this document is to help improve communications (including risk information sharing) between and among systems' cybersecurity professionals, organizations' high-level executives, and enterprises' corporate officers. The goal is to help the personnel in these enterprises and their subordinate organizations and systems to better identify, assess, and manage cybersecurity risks in the context of their broader mission and business objectives.[4] This document will help cybersecurity professionals understand what executives and corporate officers need to carry out enterprise risk management (ERM). This includes but is not limited to what data to collect, what analysis to perform, and how to consolidate lower-level risk information so that it provides usable inputs for ERM programs. This document will also help high-level executives and corporate officers understand the challenges that cybersecurity professionals face in providing them with the information they are accustomed to getting for other types of risk.

Government and private industry ERM programs are similar but often involve different oversight and reporting requirements, such as Congressional testimony versus a regulatory filing. For this reason, the Committee of Sponsoring Organizations (COSO) is often cited due to its dual role in providing guidance to both public and private organizations regarding ERM and the fact that OMB adopted much of its language when developing Circular A-123.

This document opens the discussion to bridge existing private industry risk management processes with existing government-mandated federal agency cybersecurity risk requirements. It

[4] Figure 1 depicts the correlation of cybersecurity professional (system), high-level executives without fiduciary reporting requirements (organization), and corporate officers with fiduciary reporting requirements (enterprise), respectively.

also attempts to synchronize approaches for decomposing selected concepts in subsequent documents. Concepts most likely to be addressed in more detail are those that often involve non-standard approaches, such as communicating risk, consistently identifying threats/risks, estimating likelihood and impact, calculating risk exposure, establishing and using risk reserves, monitoring risk, reporting risk, and integrating with ERM programs.

This document references some materials that are specifically intended for use by federal agencies and will be highlighted as such, but the concepts and approaches are intended to be useful for all enterprises.

1.2 Document Structure

The remainder of this document is organized into the following major sections:

- Section 2 explains the basics of ERM and cybersecurity risk management and highlights high-level gaps between current practices for ERM and cybersecurity risk management.
- Section 3 discusses cybersecurity risk considerations throughout the ERM process in detail, highlighting the use of the risk register to document cybersecurity risk as ERM input.
- Section 4 examines adopting a portfolio view of risk at the enterprise level based on normalizing and aggregating risk registers into an Enterprise Risk Register and then applying prioritization to it to generate an Enterprise Risk Profile in support of senior executive decision-making during boardroom deliberations.
- The References section lists the references for the document.
- Appendix A contains acronyms used in the document.
- Appendix B provides a glossary of terminology used in the document.
- Appendix C lists Federal Government sources for identifying risks as defined in *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2].

An Informative Reference that links the contents of this document with the NIST Cybersecurity Framework will be posted as part of the National Cybersecurity Online Informative References (OLIR) Program.[5]

[5] See https://www.nist.gov/cyberframework/informative-references for an overview of OLIR.

2 Gaps in Managing Cybersecurity Risk as an ERM Input

Office of Management and Budget (OMB) Circular A-11 defines risk as "the effect of uncertainty on objectives" [1]. The effect of uncertainty on *enterprise* mission and objectives may then be considered an "enterprise risk" that must be similarly managed. Managing risks at that enterprise level is known as enterprise risk management (ERM) and calls for understanding the core risks that an enterprise faces, determining how best to address those risks, and ensuring that the necessary actions are taken. Today's digital information and technologies impact every aspect of enterprise environments. This publication focuses on recognizing and incorporating *cybersecurity risk*[6] within the overall sphere of enterprise risk.

This approach complements other NIST documents by informing and extending existing guidance to respond to risks to an enterprise's data, information, and technology assets. Integration draws upon cybersecurity risk management and the basics of ERM, which informs and is informed by various risks at subordinate levels. Comparing the results of cybersecurity risk management activities with those required for effective input to ERM enables enterprise stakeholders to identify opportunities to close gaps.

2.1 Overview of ERM

ERM requires identifying the various types of risk that an enterprise faces, determining the probability that these risks will occur, and estimating their potential impact. OMB considers ERM to be "an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos" [1].

Cybersecurity risk is only one portion of the spectrum of an enterprise's core risks that ERM addresses. Appendix A of *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2] defines numerous risk types, including compliance, cybersecurity ("cyber information security"), financial, legal, legislative, operational, reputational, and strategic. This list can easily be expanded to all other risk disciplines, such as safety, privacy, and supply chains that ultimately anchor in ERM. In ERM, enterprises manage the combined set of enterprise risks holistically.[7]

The Committee of Sponsoring Organizations (COSO) publication, *Enterprise Risk Management—Integrating with Strategy and Performance,* defines ERM as the "culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing

---

[6] *Cybersecurity risk* is an effect of uncertainty on or within a digital context. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (Definition based on International Organization for Standardization [ISO] Guide 73 [6] and NIST Special Publication [SP] 800-60 Vol. 1 Rev. 1 [7].)

[7] "OMB Circular A-123 establishes an expectation for federal agencies to proactively consider and address risks through an integrated, organization-level view of events, conditions, or scenarios that impact mission achievement." [4]

value" [8]. Public and private enterprises have a common primary purpose for ERM: to ensure that the enterprise's mission, finances (e.g., net revenue, capital, and free cash flow), and reputation (e.g., stakeholder trust) are safeguarded in the face of natural, accidental, and adversarial threats.

This is accomplished by considering enterprise risks in relation to achieving strategic objectives (as established in the strategic plan) and operational objectives. OMB Circular A-123 requires ERM risk profiles to include four kinds of objectives: strategic, operations (operational effectiveness and efficiency), reporting (reporting reliability), and compliance (compliance with applicable laws and regulations). While there may be some overlap of risk among these categories of objectives, understanding uncertainty as it affects these objectives will help inform effective and timely decision-making. In turn, that supports risk guidance back to subordinate levels. Effective *enterprise risk management* balances achieving security objectives with optimizing limited resources. Effective *management* balances achieving enterprise mission and objectives with optimizing resources (which are often limited) and risk.

This document draws on ERM principles regarding integration with culture, strategy, and performance. One such principle is that an "organization must manage risk to strategy and business objectives in relation to its *risk appetite*—that is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value" [8]. OMB adapted this language for government use in Circular A-123 by similarly stating it "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision."

Another important ERM concept is *risk tolerance*—the organization or stakeholders' readiness to bear the remaining risk *after responding to or considering the risk* in order to achieve its objectives (while recognizing that such tolerance can be influenced by legal or regulatory requirements) [6].[8] OMB again adapted the COSO language by stating that risk tolerance "is the acceptable level of variance in performance relative to the achievement of objectives." Risk appetite is established by the organization's most senior level leadership (enterprise) and serves as the guidepost for setting strategy and selecting objectives.

Risk tolerance can be defined at the enterprise level, but OMB offers a bit of discretion to an organization, stating that it is "generally established at the program, objective, or component level" of an organization. Risk tolerance is always interpreted and applied by the receiving custodians of the risk management discipline (e.g., cybersecurity, legal, privacy) and usually interpreted at the organizational or system level [4].[9] For example, a statement of risk appetite

---

[8] Similar guidance comes from OMB Circular A-123: "Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan (See OMB Circular No. A-11, Section 230), as well as risk in relation to appropriate operational objectives. Specific objectives must be identified and documented to facilitate identification of risks to strategic, operations, reporting, and compliance." [3]

[9] NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [9] uses the term "risk tolerance" to collectively refer to what Circular A-123 and this publication differentiates into two terms: "risk tolerance" and "risk appetite." NIST SP 800-39 also uses the term "organizational culture," which "refers to the values, beliefs, and norms that influence the behaviors and actions of the senior leaders/executives and individual members of organizations. […] The organization's culture informs and even, to perhaps a large degree, defines that organization's risk management strategy." In other words, an organization's culture directly informs its risk appetite.

might be: "Email service must not be adversely impacted by cybersecurity events." An associated risk tolerance statement for this defined appetite is narrower, for instance, stating: "Risks interrupting email service for more than five minutes during core hours must be avoided."

Senior enterprise executives provide risk guidance (including advice regarding mission priority, risk appetite and tolerance guidance, and capital and operating expenses to manage known risks) to the organizations within their purview. Based on those governance structures, organization managers manage and monitor processes that properly balance the risks and resource utilization with the value created by information and technology. Individual risk tolerances add up to the enterprise's operating risk appetite, providing validation to senior executives that the enterprise is operating within the defined appetite.

The process of ERM must aid the senior enterprise executives by providing them with a portfolio view of key risks across the enterprise.[10]

2.1.1 Common Use of ERM

Public officials or corporate boards typically measure and weigh the impact and likelihood of each type of significant threat (e.g., market, operational, labor, geopolitical, cyber) to determine their individual and total impacts on the enterprise's mission, finances, and reputation. The public officials or board members then determine their risk appetite and resource allocations for each type of risk commensurate with impact and likelihood and balanced among all enterprise risk exposures. Public officials and board members also provide guidance to their corporate officers at the enterprise level and to high-level executives at the organizational level (see Figure 1). This includes guidance on ceilings for capital expenditures (CapEx) and operating expenses (OpEx) and objectives for free cash flow. They then issue guidance to continue, accelerate, reduce, delay, or cancel significant enterprise initiatives while making decisions about what constitute prudent risk disclosures that balance the competing objectives of informing stakeholders and overseers (including regulators) through required filings and statements at hearings and needing to protect sensitive information from competitors and adversaries.

2.1.2 ERM Framework Steps

There are many resources that document ERM frameworks and processes. Table 1 provides a notional crosswalk among several of these resources. They all generally include the same approaches: identify context, identify risks, analyze risk, estimate risk importance, determine and execute the risk response, and identify and respond to changes over time. The resources used in Table 1 are the ERM Playbook [2], International Organization for Standardization (ISO) 31000 [10], OMB Circular A-123 [3], and the U.S. Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book) [11]. Other resources include three of the core publications for the NIST Risk Management Framework: SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* [12]; SP 800-37, Revision 2, *Risk*

[10] This is defined by OMB as "insight into all areas of organizational exposure to risk […] thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment." [3]

Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [13]; and SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [9].

The entries in Table 1 indicate (in parentheses) their identifier or section number from the source material whenever available.

Table 1: Notional Crosswalk Among Selected ERM and Risk Management Frameworks

<table>
<tr><th rowspan="2">ERM Playbook</th><th colspan="2" rowspan="2">ISO 31000:2018</th><th rowspan="2">OMB A-123</th><th rowspan="2">GAO Green Book</th><th colspan="3">NIST Risk Management Framework</th></tr>
<tr><th>SP 800-30 Rev. 1</th><th>SP 800-37 Rev. 2</th><th>SP 800-39</th></tr>
<tr><td>Identify the Context</td><td colspan="2">Establish External Context (5.3.2), Establish Internal Context (5.3.3)</td><td>Establish Context</td><td>Define objectives and risk tolerances (6.01)</td><td>Preparing for the Risk Assessment (3.1)</td><td>Prepare (3.1)</td><td>Framing Risk (3.1)</td></tr>
<tr><td>Identify the Risks</td><td rowspan="6">Risk Assessment</td><td>Risk Identification (5.4.2)</td><td>Identify Risks</td><td>Identification of Risks (7.02)</td><td>Task 2-1: Identify and characterize threat sources of concern (3.2), Task 2-2: Identify potential threat events, threat sources (3.2), Task 2-3: Identify vulnerabilities/predisposing conditions (3.2)</td><td rowspan="3">Prepare (3.1), Task P-14, Risk Assessment - System, Risk Assessment Report (RAR)
Assess (3.5)</td><td rowspan="2">Framing Risk (3.1)</td></tr>
<tr><td>Analyze the Risks
Assess Impact
Assess Likelihood
Prioritize Risks
Calculate Exposure</td><td>Risk Analysis (5.4.3)
Calculate Level of Risk</td><td>Analyze and Evaluate</td><td>Analysis of Risks (7.05)
Management estimates the significance of a risk and considers the magnitude of impact, likelihood of occurrence, and nature of the risk</td><td>Task 2-5: Determine the adverse impacts from threat events (3.2), Task 2-4: Determine the likelihood (3.2), Task 2-6: Determine the risk to the organization (3.2)
Risk Assessment Report (Appendix K)</td><td>Assessing Risk (3.2)</td></tr>
<tr><td>Plan and Execute Response Strategies</td><td>Risk Evaluation (5.4.4)</td><td>Develop Alter-natives</td><td rowspan="2">Response to Risks (7.08)</td><td rowspan="2">Task 3-1: Communicate Risk Assessment Results
Task 3-2: Share Risk-Related Information (3.3)
Also See 800-37 Rev. 2
See 800-39</td><td>Categorize (3.2), Select (3.3), and Implement (3.4)</td><td rowspan="2">Responding to Risk (3.3)</td></tr>
<tr><td colspan="2">Risk Treatment (5.5)</td><td>Respond to Risks</td><td>Implement (3.4), Authorize (3.6), Residual Risk reflected in POA&M</td></tr>
<tr><td>Monitor, Evaluate, and Adjust</td><td colspan="2">Monitoring and review (5.6)</td><td>Monitor and Review</td><td>Identification of Change (9.02)
Analysis of and Response to Change (9.04)</td><td>Task 4-1: Conduct ongoing monitoring of the risk factors (3.4)
Task 4-2: Update Risk Assessment</td><td>Monitor (3.7)</td><td>Monitoring Risk (3.4)</td></tr>
</table>

This document utilizes the processes of the ERM Playbook [2] (column 1 in Table 1) to address cybersecurity risks. Figure 2 from the ERM Playbook depicts an example of an ERM framework. The steps in Figure 2 are used as the basis for structuring the rest of this document, but this is not

meant to imply that all enterprises should use these particular steps. Enterprises should use whatever ERM approach they favor with the assumption that it will contain the content of these steps in some way. The top row within Figure 2 depicts six steps with the arrows indicating sequence. The lower row of boxes explains the output of each step. The element at the bottom of the figure indicates that communication and consultation occur throughout all steps. Section 3 discusses each of these steps in detail:

1. **Identify the context.** Context is the environment in which the enterprise operates and is influenced by the risks involved.
2. **Identify the risks.** This means identifying the comprehensive set of positive and negative risks—that is, determining which events could enhance or impede objectives, including the risks entailed by failing to pursue an opportunity.
3. **Analyze the risks.** This involves estimating the likelihood that each identified risk event will occur and the potential impact of the consequences described.
4. **Prioritize the risks.** The exposure is calculated for each risk based on likelihood and potential impact, and the risks are then prioritized based on their exposure.
5. **Plan and execute risk response strategies.** The appropriate response is determined for each risk, with the decisions informed by risk guidance from leadership.
6. **Monitor, evaluate, and adjust.** Continual monitoring ensures that enterprise risk conditions remain within the defined risk appetite levels as cybersecurity risks change.

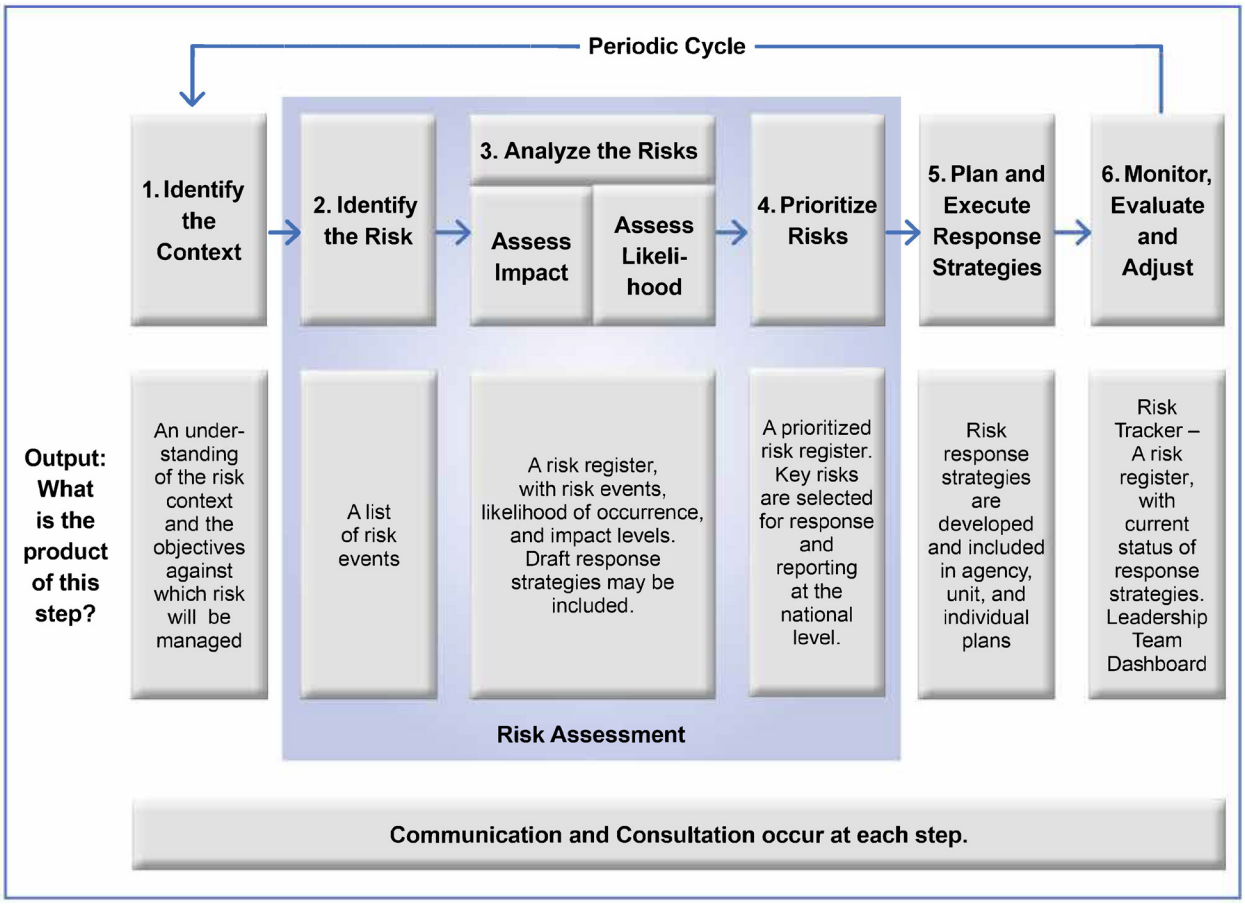


Figure 2: ERM Framework Example

OMB Circular A-123 [3] recommends (and requires for federal users) that risks be recorded in a risk register of appropriate content and format. Cybersecurity risks need to be documented and tracked in cybersecurity risk registers in order to support better management of cybersecurity risks at the enterprise level. OMB Circular A-11 describes a *risk register* as "a repository of risk information including the data understood about risks over time." It also states, "Typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks" [1]. Cybersecurity risk registers are a key aspect of managing cybersecurity risks within an enterprise. Each register evolves and matures as other risk activities take place.

Not all risk management methodologies generate an artifact called a risk register or risk log. However, the output of each methodology contains the underpinnings of or can serve as an input to a risk register. Because they are such useful information-gathering constructs, organizations not yet familiar with or using risk registers are strongly urged to adopt and integrate them into whatever risk management methodology they are currently using. Risk registers represent an organizing principle for communicating cybersecurity risks to the OMB Circular A-123 ERM process already familiar with this management construct. Their use as a shared organizing construct at the cybersecurity level ensures seamless communication and use of terminology

from the cybersecurity risk discipline to the boardroom deliberation. Section 3 of this document contains more information on cybersecurity risk registers.

There are many publications with more information on ERM fundamentals, including:

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*[11] [3]
- *Enterprise Risk Management Integrating with Strategy and Performance* [8]
- *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2]

2.2 Shortcomings of Typical Approaches to Cybersecurity Risk Management

Cybersecurity risk management follows many of the same high-level principles as the ERM framework. However, cybersecurity risk management is typically executed quite differently, and its standard outputs are often not properly conditioned as direct ERM inputs. Common reasons for these shortcomings are described below. Later parts of this document, as well as subsequent documents, will address the shortcomings.

2.2.1 Lack of Asset Information

Keeping track of an organization's computing assets, especially end user devices and data, has always been a challenge. That has been exacerbated by the proliferation of mobile devices (e.g., smartphones, tablets), the Internet of Things (IoT), cloud computing, and bring-your-own-device (BYOD), as well as the convergence of IT and operational technology (OT) systems. It is increasingly difficult to know which computing devices the organization uses and where the organization's data is stored, especially when devices and data are constantly changing. The lack of information on technology assets means it is not possible to fully quantify those assets or the impact of cybersecurity risks.

2.2.2 Lack of Standardized Measures

Cybersecurity risk measurement has been extensively researched for decades. As measurement techniques have evolved, the complexity of digital assets has also greatly increased, making the measurement problem more difficult to solve. Some low-level measures[12] have been standardized, like the estimated likelihood and impact of a particular vulnerability being exploited [14]. However, for other aspects of cybersecurity risk, there are no standard measures.

---

[11] "This Circular defines management's responsibilities for enterprise risk management (ERM) and internal control. The Circular provides updated implementation guidance to federal managers to improve accountability and effectiveness of federal programs as well as mission-support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal control into existing business activities and as an integral part of managing an agency" [4].

[12] NIST typically uses the term "measures" instead of "metrics." For more information on the distinction, see https://samate.nist.gov/index.php/Metrics_and_Measures.html.

Without consistent measures, there is little basis for analyzing risk or expressing risk in comparable ways across digital assets and the systems composed of those assets.

2.2.3 Informal Analysis Methods

Risk analysis tends to be inconsistent for cybersecurity risk management compared to many other forms of risk. Where guidance is provided, such as in NIST SP 800-30, the resulting Risk Assessment Reports (RARs) from agencies differ significantly. Moreover, foundational inputs for likelihood and impact calculations generally lack a standardized methodology or are left to the discretion of vendors who provide a scoring system. Decisions are often made based on an individual's instinct and knowledge of conventional wisdom and typical practices. For example, many security controls are automatically applied to protect a new device without first quantifying how those controls would affect risk. In addition, there is usually no analysis performed after control deployment to determine if risk has been reduced to a level deemed acceptable (i.e., within the established risk tolerance parameters).

2.2.4 Focus on the System Level

Management of cybersecurity risk is conducted in different ways at various levels, including at the system, organization, and enterprise level, as depicted in Figure 1. A common practice is for individual system-level teams to be responsible for tracking relevant risks. Typically, there is no mechanism in place to consolidate the cybersecurity risk data for systems to the organization level, much less to the enterprise level. Therefore, it is not surprising that cybersecurity risk management tends to struggle with understanding cybersecurity risk at higher levels. This may be less pronounced in organizations with an enterprise architecture that maps systems onto the business processes they support.

While this report focuses on cybersecurity risks as they contribute to ERM, many enterprise risks are interdependent. A common industry example is that while cybersecurity risk and credit risk are different elements of the ERM portfolio, it is quite possible that a cybersecurity breach could result in a credit downgrade or a loss of public confidence. Because of these interdependencies, it is important that enterprise managers collaborate, communicate, and recognize that information and technology risks are not isolated issues.

2.2.5 Increasing System and Ecosystem Complexity

Many systems upon which agencies and institutions rely are complex, adaptive "systems-of-systems" composed of thousands of interdependent components and myriad channels. They operate in a rapidly changing socio-political-technological environment that presents threats from individuals and groups with shifting alliances, attitudes, and agendas.

The constant introduction of new technologies has changed and complicated cyberspace. Wireless connections, big data, cloud computing, and IoT present new complexities and concomitant vulnerabilities. Information and technology no longer represent the simple, automated filing system. Rather, they are like the central nervous system—a delicately balanced and intricate part of any organization or enterprise that coordinates and controls the most

fundamental assets of most organizations. This ecosystem's increasing complexity gives rise to systemic risks and exploitable vulnerabilities that, once triggered, can have a runaway effect with multiple, severe consequences for enterprises and the Nation. Managing cybersecurity risk for these ecosystems is incredibly challenging because of their dynamic complexity.

This complexity brings risk to specific systems and their technical vulnerabilities, which then extend to entire systems, organizations, and enterprises. Moreover, emerging risk conditions created by the interdependence of systems must also be identified, tracked, and managed.

> More information on cybersecurity risk management is available from numerous NIST documents, including SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [13] and the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [15]. They reference a "risk-based approach," which enables an organization to determine the risks that are relevant to its mission throughout the operational life cycle and to apply appropriate resources to respond to those risks to an acceptable level. Implementation of such an approach will vary depending upon the relevant stakeholders' risk appetite, risk tolerance, and available resources.
>
> Note that while the focus of this publication is cybersecurity risk, its high-level approaches should also be relevant for privacy risk. See *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* for a privacy risk management approach [16].

2.3 The Gap Between Cybersecurity Risk Management Output and ERM Input

At its core, managing cybersecurity risk means balancing the benefit of applying information and technology with the potential negative impact and likelihood of the consequences of that application being deployed at the system, organization, or enterprise level. An enterprise that avoids all cybersecurity risk might stifle innovation or efficiencies to the point where little value would be produced. At the other end of the spectrum, an enterprise that applies technology without regard to cybersecurity risk increases the chances that it might fall victim to undesirable consequences. Effectively balancing the benefits of technology with the potential consequences of a threat event will result in effective cybersecurity risk management that supports a comprehensive ERM approach. Cybersecurity risk officers should consider the influence of cybersecurity risks on achieving the above-referenced enterprise strategic, operations, reporting, and compliance objectives. Enterprise Risk Officers should consider communicating these enterprise objectives so that cybersecurity risk officers can take actions at lower levels and escalate relevant risk inputs to ERM programs. These Enterprise Risk Officers also need to take into account relevant policy decisions and regulatory impacts.

For ERM purposes, each system[13] and organization should have a cybersecurity risk register that is primarily informed by the enterprise's cybersecurity objectives. At higher levels in the enterprise, the contents of those registers will be aggregated, normalized, and prioritized. This allows for easy transfer of cybersecurity risk knowledge from cybersecurity risk management to

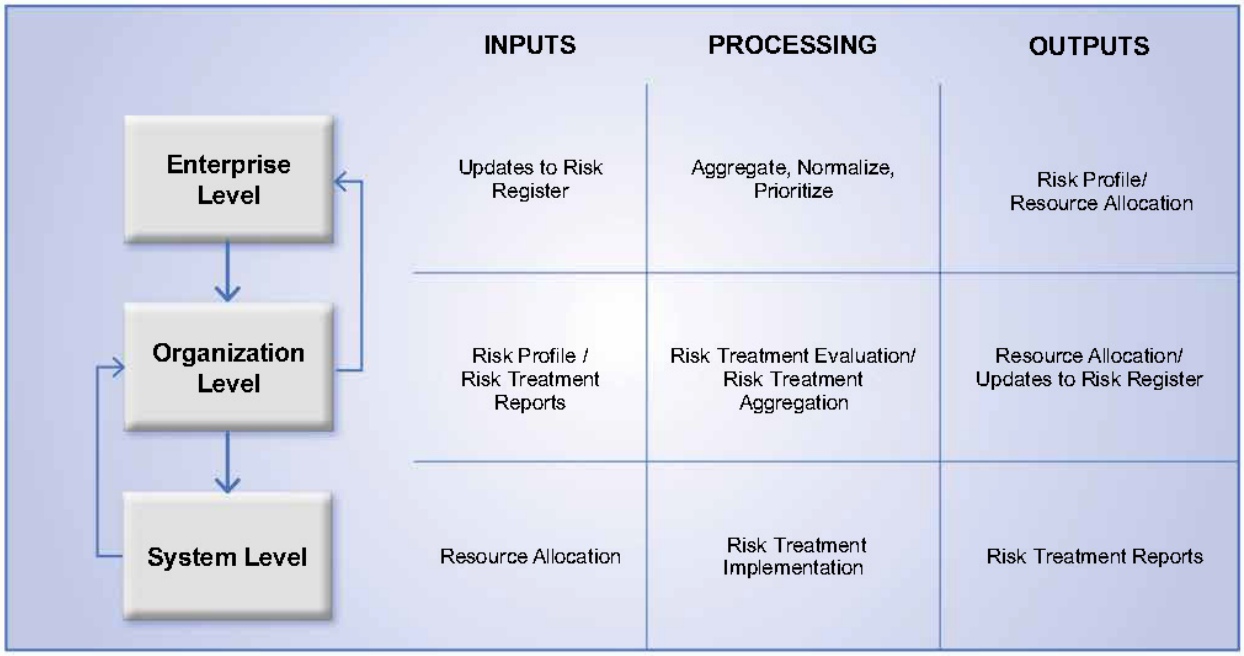
[13] OMB Circular A-130 defines an *information system* as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

ERM. Figure 3 highlights the flow of information. To condition cybersecurity risk data to better align with enterprise risk, organizations should utilize a cybersecurity risk register for these risk management activities:

1. Aggregate risks from adversary threats and system failures that result in compromised information. *Aggregation* is the consolidation of similar or related information.
2. Normalize information across organizational units to provide enterprise executives with the information needed to measure cybersecurity risks that would affect enterprise objectives. *Normalization* is the conversion of information into consistent representations and categorizations.
3. Prioritize operational risk treatment activities by combining risk information with enterprise mission and budgetary guidance to implement appropriate responses.

Currently, many organizations do not provide these activities in consistent, repeatable ways. Methods such as quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are largely ad hoc and not performed with the rigor used for other types of risk.[14] Improving the risk measurement and analysis methods used in cybersecurity risk management, along with widely using cybersecurity risk registers, would improve the quality of the risk information provided to ERM, which promotes better management of cybersecurity risk at the enterprise level and supports enterprises.

[14] The NIST Cybersecurity Framework [16] describes this cybersecurity risk management disparity as a progression through the four Tiers—Partial, Risk Informed, Repeatable, and Adaptive—where risk management processes mature from ad hoc to formalized and agile.



671

672 **Figure 3: Information Flow Between System, Organization, and Enterprise Levels**

673 According to NISTIR 8170, *Approaches for Federal Agencies to Use the Cybersecurity*
674 *Framework*, enterprises "develop policies to identify, assess, and mitigate adverse effects with
675 cybersecurity dependencies across various types of enterprise risks. […] Many of these other
676 types of risk may also have cybersecurity risk implications or be impacted by cybersecurity.
677 Some employ different terminologies and risk management approaches to make decisions. […]
678 Organizations may have established a unique lexicon for ERM that should be considered when
679 communicating risks. […] This necessitates coordination with existing ERM functions on how to
680 best incorporate and communicate cybersecurity risks at the organization and system levels" [4].

3 Cybersecurity Risk Considerations Throughout the ERM Process

Using cybersecurity risk registers provides consistency in the capture and communication of risk-related information throughout the ERM process. The risk register is first used to identify relevant risk scenarios. It then provides a framework for organizing and communicating risk information from the individual system level up through the organizational level and finally to the highest enterprise level. The risk registers used at each level convey information about risk assessments, evaluation decisions, responses, and monitoring activities.

As introduced in previous sections, a key goal of cybersecurity risk management is to help enterprise stakeholders optimize risk and resources to support enterprise business objectives. The information and technology being secured provide value to the enterprise by supporting one or more business needs. The cybersecurity risk management process is intended to help ensure that the enterprise can realize that value while achieving stakeholders' expectations regarding the protection of confidentiality, integrity, and availability. Each of the following stages of cybersecurity risk management as an ERM input should be based on the potential impact of a given risk scenario on the enterprise and mission and business objectives.

This section references two types of controls in support of ERM, each of which is essential and should not be confused:

- **Internal Controls** are the overarching mechanisms used to achieve and monitor enterprise objectives. The COSO Internal Control – Integrated Framework defines internal control as "a process effected by an entity's board of directors, management and other personnel designed to provide reasonable assurance of the achievement of objectives" [17]. These internal controls are an important factor at the enterprise level. In fact, the title of OMB Circular A-123 is "Management's Responsibility for Enterprise Risk Management and Internal Control."
- **Security Controls** operate at a lower level and represent the "safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information." Security (and privacy) controls provide the management, administrative, and technical methods for responding to cybersecurity risks by deterring, detecting, preventing, or correcting threats and vulnerabilities.

Figure 4 shows a notional cybersecurity risk register template. The remainder of Section 3 provides guidance and useful information for completing and using cybersecurity risk registers and integrating them with ERM. The notional template includes many of the elements suggested by OMB Circular A-11, which states that "typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks" [1].

Notional Cybersecurity Risk Register											
				Current Assessment							
ID	Priority	Risk Description	Risk Category	Impact	Likelihood	Exposure Rating	Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
1											
2											
3											
4											
5											
Continually Communicate, Learn and Update											

Figure 4: Notional Cybersecurity Risk Register Template[15]

Table 2 describes each of the elements in the notional cybersecurity risk register template.

Table 2: Descriptions of Notional Cybersecurity Risk Register Template Elements

Register Element	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register (e.g., 1, 2, 3)
Priority	A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low)
Risk Description	A brief explanation of the cybersecurity risk scenario impacting the organization and enterprise. Risk descriptions are often written in a cause and effect format, such as "if X occurs, then Y happens."
Risk Category	An organizing construct that enables multiple risk register entries to be consolidated (e.g., using SP 800-53 Control Families: Access Control (AC), Audit and Accountability [AU] as illustrated in Figure 6). This value is important for comparing across risk registers during the risk aggregation step of ERM.
Current Assessment—Likelihood	An estimation of the probability, before any risk response, that this scenario will occur. On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Current Assessment—Impact	Analysis of the potential benefits or consequences resulting from this scenario if no additional response is provided. On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Current Assessment—Exposure Rating	A calculation of the likely risk exposure based on the inherent likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as *exposure*. Other common frameworks use different terms for this combination, such as *level of risk* (ISO 31000, NIST SP 800-30 Rev. 1). On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Risk Response Type	The risk response (sometimes referred to as the risk strategy or risk treatment) for handling the identified risk. Values for risk response types are listed in Table 3 and Table 5 of this document.
Risk Response Cost	The estimated cost of applying the risk response

Register Element	Description
Risk Response Description	A brief prose description of the risk response. The NIST Cybersecurity Framework Subcategory outcomes can be adapted to help populate the Risk Response Description field of the cybersecurity risk register where appropriate (e.g., ID.AM-2: Software platforms and applications within the organization are inventoried, ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources) as illustrated in Figure 6.
Risk Owner	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The Risk Owner may work with a designated Risk Manager who is responsible for managing and monitoring the selected risk response
Status	A field for tracking the current condition of this risk and any next activities

This section discusses how risk registers are used within organizations and how a risk register's contents are prioritized to serve as the basis of a risk profile. Section 4 explains what happens at the enterprise level when the risk profiles of its organizations are correlated, aggregated, normalized, and deconflicted, with the key risks compiled into the Enterprise Risk Profile (such as the Agency Risk Profile described in OMB Circular A-123 Section B1) [3].

It is noteworthy that the risk register model shown here illustrates a single point in time. The actual composition of the register will vary among enterprises and may contain more or fewer data points than those described in Table 2. For example, some organizations may wish to include both the current risk assessment (before risk response is applied) and the target residual risk assessment that is expected to result from the risk response.

Regardless of which model is selected for use as a risk register, it is important for the enterprise to ensure that the model is used in a consistent and iterative way. As the risk professional progresses through the steps in Section 3, the risk register will be populated with relevant information. Once decisions have been made as part of a subsequent review of the risks, the agreed-upon risk response becomes the current state, and the cycle begins anew.

While the risk register itself can be used to document and communicate information about current risks and their treatment, it may be necessary to supplement the register with a risk detail record. This detailed risk record may be stored and maintained in a written record, as part of an organizational knowledge management system, or as a database entry in risk-specific software such as a Governance/Risk/Compliance (GRC) application. The use of such a template enables the documentation of details regarding the considerations, assumptions, and results of risk activity. It also enables the enterprise to record personnel involved in those considerations, any actions to be taken, and schedules. Contents of a detailed risk record may include:

- Information regarding the risk itself, such as a detailed risk scenario description and underlying threats, vulnerabilities, assets threatened, risk category, and risk assessment results
- Roles involved in risk decisions and management (e.g., risk owner, risk manager, action owner for specific activities, stakeholders involved in risk treatment decisions, contractual agreements for supply chain/external partners)

- Schedule considerations, such as the date the risk was first documented, the date of the last risk assessment, and the date of the next expected assessment
- Risk response decisions and follow-up, including detailed plans, status, and risk indicators

The examples above only illustrate the current risk assessment (i.e., likelihood, impact, and resulting exposure value). Each organization may find it helpful to determine which assessments are helpful to reflect in its risk register. This report describes the risk register as an input into the risk management decision process, so only the current risk assessment results are depicted. An organization could also choose to include the *Target Risk Assessment*, reflecting the changes to likelihood, impact, and exposure that are anticipated to result from the recommended risk response. If the register is to be updated after the actual risk response, the results of a post-response assessment could be reflected in the register as the actual *Residual Risk Assessment*. Because the risk management process is iterative, the assessment will change as the risk management life cycle continues.

NIST SP 800-30, Revision 1, Appendix K [12] describes relevant cybersecurity risk elements that might be recorded in what is called a *cybersecurity risk assessment report (RAR)*, which provides a detailed record of the planning and execution of an evaluation of a relevant set of risks. Elements that match those described in Table 2 of this document might be added to cybersecurity risk registers, and creating a cybersecurity RAR can be considered a prerequisite to creating a cybersecurity risk register. Doing so would allow those seeking additional information about a given cybersecurity risk register entry to readily find such information recorded in the corresponding RAR.

3.1 Identify the Context

The first step in managing cybersecurity risks to the organization is understanding *context*—the environment in which the organization operates and is influenced by the risks involved. As shown in Figure 4, the context is not directly recorded in the cybersecurity risk register, but it provides important input into that register by documenting the expectations and drivers to be considered in the register's development and maintenance. The risk context includes two factors:

- **External context** involves the expectations of outside stakeholders that affect and are affected by the organization, such as customers, regulators, and business partners. These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored.
- **Internal context** relates to many of the factors within the organization and relevant cybersecurity considerations across the enterprise. This includes any internal factors that influence cybersecurity risk management, such as the organization and enterprise's objectives, governance, culture, risk appetite, risk tolerances, policies, and practices.

Several NIST frameworks begin with determining these context factors. For example, the Risk Management Framework [13] includes a *Prepare* step to identify organization strategy, management methods, and roles. Similarly, NIST Cybersecurity Framework Step 1: *Prioritize*

and Scope states, "organizations make strategic decisions regarding cybersecurity implementations and determine the scope of the systems and assets that support the selected business line or process." These context exercises identify organization mission drivers and priorities used for subsequent assessment and planning.

3.1.1 Risk Management Roles

An important element of the internal and external context is identifying the relevant work roles for each stage. Defining the types of stakeholders and recording the names of personnel in those roles involved at each stage will support risk communication and timely decision-making. (This activity supports an important outcome from the Cybersecurity Framework subcategory ID.GV-2: "Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.")

Roles described in Sections 3 and 4 of this publication include internal and external individuals and groups related to the RMF-defined Cybersecurity Risk Executive Function[16], such as:

- Cybersecurity Risk Officer – Manages the risk management process for a given information system (or set of systems). This individual may act as the Risk Owner for a particular risk in the register or as the Risk Manager designated by the Risk Owner who remains accountable for management and communication about the risk.
- Enterprise Risk Officer – A senior-level official accountable for managing and communicating risk across the enterprise. In some organizations, this may be the Chief Risk Officer (CRO) or another senior designee.
- Other C-Suite Member – Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), Chief Financial Officer (CFO), etc.
- Senior Enterprise Leaders – Agency or corporate officials, such as those who represent various elements of the organization and assist with managing and communicating risk throughout the enterprise.
- Enterprise Risk Steering Committee (ERSC) – A group responsible for receiving risk management information from throughout the enterprise and considering the overarching impact.
- Auditor – Provides independent and formal verification regarding the achievement of enterprise risk objectives and the application of enterprise risk management processes.

[16] According to the ERM Playbook, the Senior Accountable Official for Risk Management (SAORM) is the head of agency and is responsible for oversight of both information security and privacy risk management processes as well as broader enterprise risk management processes. The Risk Executive function for each domain oversees the management of risks within those domains. The Risk Executive function for cyber would be the Cybersecurity Risk Officer defined in this list, and for enterprise-level ERM would be the Enterprise Risk Officer defined in this list, in tandem with the ERM Council/Steering Committee or other governing body. A similar committee-style governance function also exists in the cybersecurity space, in the form of the CIO and CISO councils.

- Other Internal Partners – Includes other enterprise stakeholders (e.g., legal affairs, human resources, business managers) with an interest in the risk management and risk decisions performed.
- External Stakeholders – Includes external parties with an interest in the management of the enterprise's risk to an acceptable level.
- External Partners – Personnel or organizations (e.g., service providers, vendors, organizations that collaborate under a formal agreement) external to the enterprise that participate in the management and communication of cybersecurity risk.

Throughout the risk management cycle, tracked and managed by the use of cybersecurity risk registers and risk profiles, two-way stakeholder communications are critical to providing direction that enables cybersecurity risk officers[17] to identify and propose ways to manage relevant cybersecurity risks, as described in Section 3.2.

External stakeholders and partners have key roles in identifying, managing, communicating, and monitoring cybersecurity risks. Enterprises are increasingly interdependent on external partners, such as material suppliers, communications and technology providers, cloud service providers, and managed service providers. NIST recommends the use of cyber supply chain risk management (C-SCRM) plans and activities to ensure that external partners are well-integrated.[18]

3.1.2 Risk Management Strategy

A key responsibility of each level of governance is the establishment of clear and actionable risk management guidance to be used. Leaders at each level should clearly express expectations regarding enterprise risk appetite, risk tolerance, and risk capacity (described in Section 2). These values represent an enterprise risk strategy to ensuring that various risks are managed to an acceptable level. As the risk landscape evolves due to technological and environmental changes, enterprise leaders should continually review and, if needed, adjust the risk strategy. For example, an enterprise subject to outside regulation is likely to receive specific guidance from that authority regarding criteria that must be considered in evaluating acceptable risk.

Several categories in the Cybersecurity Framework describe outcomes related to effective risk management strategy and may be helpful for establishing enterprise context. The following outcomes are necessary to inform cybersecurity risk managers regarding how to identify risk scenarios, properly analyze those risks, and respond to and monitor them:

- ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

---

[17] The cybersecurity risk officer has the expertise to identify relevant cybersecurity risks as opposed to an enterprise risk officer who would receive reports on such risks. The importance of the cybersecurity risk officer role is increasingly being recognized.

[18] For more information on C-SCRM, see https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.

- ID.RM-2: Organizational risk tolerance is determined and clearly expressed.
- ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.

A critical element of the enterprise risk strategy includes consideration of supply chain risks, such as those described in the Cybersecurity Framework's Supply Chain Risk Management (ID.SC) category. While all of the ID.SC subcategories may be relevant, ID.SC-1 directly influences the enterprise risk strategy:

> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.

Assumptions may occur at all levels of the organization, so it is important to determine internal and external stakeholders' expectations regarding risk communications. Those may include strategic objectives, organizational priorities, decision-making processes, and risk reporting/tracking methodologies (e.g., regular risk management committee discussions and meetings).

An effective ERM program defines and communicates enterprise risk appetite. It serves as a guidepost and reflects strategic risk direction from leadership. As adopted from COSO, OMB Circular A-123 defines risk appetite as "the broad-based amount an enterprise is willing to accept in pursuit of its mission/vision." With strategic risk direction communicated to the system and organizational levels of the enterprise, cybersecurity officers can apply the guideline at system and organization levels when establishing risk expectations at those levels. Strategic risk direction from leadership usually includes guidance regarding risk appetite and risk tolerance, such as acceptable levels of risk at the system and organization levels. Risk guidance can also include direction regarding how risk register entries should be categorized. The use of common risk categories supports the aggregation of various types of risk, such as ordered by the nature of the risk (e.g., supplier risks, access management risks) or by analysis results (e.g., high risks, risks to payroll).

In providing risk strategy direction, it is critical that enterprise leaders also provide guidance regarding risk calculations. Establishing a common scale for assessing levels of risk will support consistent risk estimation, measurement, and reporting. The strategy may also include guidance regarding the mechanisms and frequency of risk reporting.

As cybersecurity risks are recorded, tracked, and reassessed throughout the risk life cycle, this foundation ensures that all agree about how various types of risk will be communicated, managed, and escalated to ensure adherence to risk guidance and expectations.

3.2 Identify the Risks

The second step in Figure 2 involves identifying a comprehensive set of risks and recording them in the risk register. This involves determining which events could enhance or impede objectives,

including the risks involved in failing to pursue opportunities. Circular A-123 [3] requires that the risk register consider both inherent and residual risk. Those terms are described in the following ways [8]:

- "Inherent risk is the risk to an entity in the absence of any direct or focused actions by management to alter its severity."
- "Target residual risk is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk."
- "Actual residual risk is the risk remaining after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk."

Cybersecurity risk identification is comprised of four inputs, which are discussed in more detail below:

- Identification of the organization's relevant assets and their valuation;
- Determination of potential information and technology opportunities that might benefit the organization and potential threats that might jeopardize the confidentiality, integrity, and availability of those assets;
- Consideration of the vulnerabilities of those assets; and
- High-level evaluation of potential consequences of risk scenarios.

3.2.1 Inventory and Valuation of Assets

The Cybersecurity Framework describes *assets* as "the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes" [15]. An asset could be a communications circuit, a staff member, or a piece of information, such as intellectual property. A potential impact on assets cannot be determined without a comprehensive asset inventory, so that inventory is often among the first inputs needed. Such an inventory should also provide a method for tracking the owner/manager of each asset and the asset's relative importance (or value). Without a clear account of the technology assets, it is not possible to fully quantify information assets or the impact of cyber risks being realized on said assets.

Increasingly, many of the assets on which an organization depends are not within its direct control. External technical assets may include cloud-based software or platform services, telecommunications circuits, and video monitoring. Personnel may include the internal workforce, external service providers, and third-party partners, as described in Section 3.1.

A core ERM concept is prioritizing attention and resources towards those assets that have the greatest impact on an enterprise's ability to achieve its mission (and, in the case of federal agencies, impact that affects the public.) Accordingly, federal agencies are required to identify and prioritize high-value assets (HVAs) or "critical assets." In this way, cybersecurity risk is optimized; those risks that affect the most valuable resources are assigned the largest risk exposure value.

3.2.2 Determination of Potential Threats

Cybersecurity risk is not inherently good or bad. Rather, it represents the effect of uncertain circumstances, so enterprise risk managers should consider a broad array of potential positive and negative risks. The following sections primarily deal with negative risks. Additional information about balancing them with positive risks and opportunities is provided in Section 3.7.

A *threat* represents any circumstance or event with the potential to adversely impact organizational operations (a *negative risk*). The threat could arise from a malicious person with harmful intent or from an unintended or unavoidable situation (e.g., a natural disaster, technical failure, or certain human errors) that may trigger a vulnerability.

SWOT Analysis

One commonly used method that should be employed by all organizations for identifying potential cybersecurity risk outcomes is a SWOT (strengths, weaknesses, opportunities, threats) analysis. Applying a SWOT analysis helps users identify opportunities that arise from organizational strengths (e.g., a well-respected software development team) and threats (e.g., supply chain issues) that reflect an organizational weakness. The use of SWOT analysis helps the organization describe and consider the context described in Section 3.1, including internal factors (the strengths and weaknesses internal to the organization), external factors (the opportunities and threats presented by the external environment), and ways in which these factors relate to each other.

While it is critical that enterprises address potential negative impacts on mission and business objectives, it is equally critical (and required for federal agencies) that enterprises plan for success. OMB states in Circular A-123 that "the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)." However, the notion of "planning for success" by identifying and realizing positive risks (opportunities) is a relatively new concept in cybersecurity risk management that is influencing other risk management disciplines. For the moment, it should be noted that both positive and negative risks follow the same processes from identification to calculation to inclusion on the Enterprise Risk Profile.

Weaknesses Leading to or Exacerbating Threats

Certain weaknesses—such as software flaws, missing patches, misconfigurations, and the presence of malware—can be identified using automated scanners. While these automated techniques may be insufficient to fully address targeted attacks and Advanced Persistent Threats (APTs), they represent a way to quickly identify common vulnerabilities. However, cybersecurity weaknesses are not limited simply to the hardware and software of an enterprise. Reviewing the NIST SP 800-53 controls immediately highlights the breadth of potential threats germane to cybersecurity, such as those resulting from a lack of risk planning associated with Continuity of Operations (COOP), training, monitoring physical access, power considerations, and supply chain considerations.

The NIST Cybersecurity Framework [15] also provides an excellent method for identifying weaknesses in the face of threats. *Step 6: Determine, Analyze, and Prioritize Gaps* analyzes the gaps between the organization's Current Profile (Step 3) and Target Profile (Step 5) to identify any weaknesses represented by the current state compared to the desired state. The Cybersecurity Framework includes steps for creating a high-level description of the inherent conditions for a given enterprise or organization (a current-state profile), which can also be assessed to determine threat scenarios.[19]

Numerous threat modeling techniques are available for analyzing cybersecurity-specific threats.[20] It may be helpful to consider both a top-down approach (i.e., reviewing critical/sensitive assets for what could potentially go wrong, regardless of threat source) and a bottom-up approach (i.e., considering the potential impact of a given set of threat/vulnerability scenarios). For example, the Software Engineering Institute's (SEI) OCTAVE® uses the top-down approach to help produce a catalog of potential harmful outcomes based on the effects of various threat sources and their motives [18]. Other threat modeling techniques, such as MITRE's ATT&CK™ [19], provide a knowledge base of adversary tactics and techniques based on real-world observations. There are numerous industry sources of cybersecurity-specific threat information, including commercial and non-profit organizations and public-sector sources like the United States Computer Emergency Readiness Team (US-CERT).

An extensive amount of information has already been published regarding the identification of internal and external threats. In building a register of potential cybersecurity risks, the organization should consider those negative risks events that have already occurred in similar organizations. For example, the U.S. Securities and Exchange Commission (SEC) has stated: "Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, **including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack** [emphasis added]" [20].

Whatever means are used to determine potential threats, it is important to consider them in terms of both the *threat actors* (the instigators of risks with the capability to do harm) acting on the threat sources and the *threat events* caused by their actions.

Combinations of multiple risks should also be considered. For example, if one risk in the register refers to a website outage and another risk refers to an outage of the customer help desk, there may need to be a third risk in the register that considers the likelihood and impact of an outage affecting **both** services at once. It is also important to identify cascading risks where one primary

---

[19] Given the similar pedigree of the NIST Cybersecurity Framework and the NIST Privacy Framework [17], it is by design that application of the two frameworks use the same methodology.

[20] This section is intended to introduce the topic of cybersecurity threats in the context of the enterprise. A future publication (NIST IR 8286A) will decompose cybersecurity threats and threat modeling with practical and actionable guidance as related to populating the cybersecurity risk register.

risk event may trigger a secondary and even a tertiary event. Analysis of the likelihood and impact of these first-, second-, and third-order risks is described in Section 3.3.

It is important for the Cybersecurity Risk Officer to look out for and mitigate instances of cognitive bias in risk identification. Some common issues from bias include:

- **Overconfidence** – the tendency for stakeholders to be overly optimistic about either the potential benefits of an opportunity or the ability to handle a threat
- **Group Think** – making decisions as a group in a way that discourages creativity or individual responsibility; the Delphi Technique is helpful in circumventing this pitfall
- **Following Trends** – blindly following the latest hype or craze without a detailed analysis of the specific benefit to the organization
- **Availability Bias** – the tendency to focus on issues that come readily to mind because one has heard about or read about them, perhaps in ways not representative of the issues' actual likelihood

3.2.3 Determination of Exploitable and Susceptible Conditions

The next key input to risk identification is understanding the potential conditions that enable the risk event to occur. It is important to consider all types of vulnerabilities in all assets, including people, facilities, and information. For the purposes of this document, *vulnerability* is simply a condition that enables a threat event to occur; it could be an unpatched software flaw, a system configuration error, a person who is susceptible to malicious persuasion, or a physical condition (like a wooden structure being flammable). The presence of a vulnerability does not cause harm in and of itself, as there needs to be a threat present to exploit it. Moreover, a threat that does not have a corresponding vulnerability may not result in a negative risk. Identification of negative risks includes understanding the potential threats and vulnerabilities to organizational assets, which can then be used to develop scenarios that describe potential risks.

3.2.4 Evaluation of Potential Consequences

The final component of risk identification is documenting the potential consequences of each risk listed in the register. Many organizations incorrectly express risks outside of their context. For example, a stakeholder might say, "I'm worried about floods," or "I'm concerned about a denial-of-service attack." These examples cannot be analyzed or considered without knowing the full picture. Considering the above factors, an effective example of an identified risk in cause and effect terminology might be, "If a hurricane causes a storm surge, then it could flood the data center and damage multiple critical file servers." Cybersecurity risks that cause unexpected or unreliable behavior in a system do not always result in the failure of an information system to fulfill its duty in support of the business objectives. Many of the elements of a security plan are implemented to support redundancy and resilience so that a highly likely threat event might result in manageable consequences. Resilient enterprise systems may be able to continue operating in the face of adverse circumstances.

Cybersecurity risk officers should consider and document the potential consequences of each risk listed on a cybersecurity risk register, considering all levels: system, organization, and enterprise.

3.3 Analyze the Risks

In Step 3 of Figure 2, each risk in the cybersecurity risk register is analyzed to estimate the likelihood that the risk event will occur and the potential impact of the consequences described.

3.3.1 Risk Analysis Types

As described in Section 2.2.3, relying solely on an informal analysis of risk factors may impair effective decision support for cybersecurity risk management. To aid in more accurate estimation, a broad array of risk analysis methodologies are available, including NIST SP 800-30 [12] and those described in International Electrotechnical Commission (IEC) 31010:2019 [21]. Methods for risk analysis include:

- *Qualitative analysis* is based on the assignment of a descriptor, such as low, medium, or high. The scale can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks. Qualitative analysis is helpful as an initial assessment or when intangible aspects of risk are to be considered.

  To improve the quality of qualitative analysis, values and data can be leveraged from external sources, such as industry benchmarks or standards, metrics from similar previous risk scenarios, or findings from inspections and assessments.

- *Quantitative analysis* involves numerical values, which are assigned to both impact and likelihood. These values are based on statistical probabilities and a monetized valuation of loss or gain. The quality of the analysis depends on the accuracy of the assigned values and the validity of the statistical models used. Consequences may be expressed in terms of financial, technical, or human impacts.

NIST SP 800-30, Revision 1, describes a *semi-quantitative* assessment that employs "a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts." Application of this model helps translate risk analysis into qualitative terms that support risk communications for decision-makers while also supporting relative comparisons (such as within a particular scale or bin).

Each of these analysis types has advantages and disadvantages, so the type performed should be consistent with the context associated with the risk. The methods to be selected and under what circumstances depend on many organizational factors and might be included in the risk management discussions described in Section 3.1. While qualitative methods are commonplace, the cybersecurity risk officer may benefit from considering a more quantitative methodology with a more scientific approach to estimating likelihood and the impact of consequences. This may help to better prioritize risks or to prepare more accurate risk exposure forecasts. The benefits of such an approach may be offset by the fact that changing the risk assessment methodology may require time and resources for development and training.

Common ERM practices include both qualitative and quantitative types of risk analysis. When selecting the most appropriate type of risk analysis at the system or organization level, cybersecurity risk officers should consider both consistency with ERM at the enterprise level and the accuracy of measuring cybersecurity risks.

A detailed consideration of risk analysis techniques, including worked examples, will be provided in a subsequent NIST publication.

3.3.2 Techniques for Estimating Likelihood and Impact of Consequences

Since one of the primary goals of cybersecurity risk management is to identify potential risks that are most likely to have a significant impact, accurate reflection of risk factors is critical. Fortunately, risk management has been practiced for many years, and there are many effective techniques for analyzing risk in comparison with enterprise risk appetite and system or organizational risk tolerance. IEC 31010 is an international standard that describes and provides guidance on 17 different risk assessment techniques that can be used for analyzing controls, dependencies, and interactions; understanding consequence and likelihood; and measuring overall risk [21]. An estimation of risk levels (or exposure) employs a combination of analysis methods. In addition to modeling techniques like those described below, understanding likelihood and potential impacts will also draw upon experimentation, investigation into previous risk events, and research into risk experiences of similar organizations.

The likelihood and impact elements of a risk can be broken into subfactors. For example, consider a risk scenario in which a critical business server becomes unavailable for use by an organization's financial department. The age of the server, the network on which it resides, and the reliability of its software all influence the likelihood of a failure. The impact of this scenario can also be considered through various factors. If another server is highly available through a fault-tolerant connection, the loss of the initial server may have little consequence. Other factors also impact risk analysis, such as timing. If the financial server supports an important payroll function, the impact of a loss occurring shortly before payday may be significantly higher than if it were to occur after paychecks are distributed. Impact may vary greatly depending on whether the server is used for archiving legacy records or for performing urgent stock trades. This illustration demonstrates that there are many considerations that go into estimating exposure and the events that can trigger them. Whichever sub-factors an organization chooses to consider, they should be clearly delineated and defined to ensure consistency in their use for likelihood and frequency estimation and overall risk register assessment and aggregation.

Calculation of multiple or cascading impacts is an important consideration, and each permutation should be individually included in the cybersecurity risk register. Secondary loss events should be captured with primary loss events to represent the total impact and cost of a risk scenario. Omission of secondary losses in the assessment of a risk scenario would underestimate the total impact, thereby misinforming risk response selection and prioritization. For example, while the organization might consider a risk that a telecommunications outage would result in the loss of availability of a critical web server, there may also be secondary loss events, including loss of customers from frustration with unavailable services or penalties resulting from the failure to

meet contractual service levels. An analysis of cascading risks should include the consideration of factors that would lead to a secondary risk, such as the outage described above.

Examples of techniques for estimating the probability that a risk event will occur include:

- **Bayesian Analysis** – a model that helps inform a statistical understanding of probability as more evidence or information becomes available
- **Monte-Carlo** – a simulation model that draws upon random sample values from a given set of inputs, performs calculations to determine results, and iteratively repeats the process to build up a distribution of the results
- **Event Tree Analysis** – a modeling technique that represents a set of potential events that could arise following an initiating event from which quantifiable probabilities could be considered graphically

Both tangible (e.g., direct financial losses) and less tangible impacts (e.g., reputational damage and impairment of mission) should be considered when evaluating the potential consequences of risk events. These are connected since direct losses will affect reputation, and reputational risk events will nearly always result in risk response expenses. OMB Circular A-123 states that "reputational risk damages the reputation of an Agency or component of an Agency to the point of having a detrimental effect capable of affecting the Agency's ability to carry out mission objectives" [3]. There is a broad range of stakeholders to be considered when estimating reputational risk, including workforce, partners, suppliers, regulators, legislators, public constituents, and clients/customers.

Cybersecurity risk officers document and track the potential consequences of each cybersecurity risk that would significantly impact enterprise objectives, such as causing material reputation damage or significant financial losses to the enterprise. Documenting and tracking these consequences at the organization or system level streamlines the step of providing cybersecurity risk inputs to the ERM program discussed in Section 3.8.

The estimation of the likelihood and impact of a risk event should account for existing and planned controls. The ERM Playbook [2] provides the following guidance:

> "Identifying existing controls is an important step in the risk analysis process. Internal controls (such as separation of duties or conducting robust testing before introducing new software) can reduce the likelihood of a risk materializing and the impact. […] One way to estimate the effect of a control is to consider how it reduces the threat likelihood and how effective it is against exploiting vulnerabilities and the impact of threats. Execution is key—the presence of internal controls does not mean they are necessarily effective."

The estimated impact and likelihood for each risk are recorded in the inherent impact and likelihood columns within the cybersecurity risk register. After risk responses are determined, the analysis should be revised to adjust each risk impact and likelihood to reflect the amount of impact or likelihood mitigation that accrues from each risk response. The residual risk (i.e., the amount of risk that remains after risk responses are applied) should then be recorded in the risk

register's Residual Risk column. To simplify the process of normalizing cybersecurity risk registers when developing an enterprise risk register (see Section 3.8), a consistent time frame should be used for estimating the likelihood of each risk. Likewise, the level of impact value assists with normalizing the risk during the aggregation and prioritization process.

3.4 Prioritize Risks

After identifying and analyzing applicable risks and recording them in the cybersecurity risk register, a cybersecurity risk profile should be created from the risk register. This is accomplished by prioritizing the identified risks based on exposure and selecting which ones exceed the risk acceptance criteria. That includes identifying who will make such determinations. If a risk has a likely impact with enterprise consequences (such as impacting key strategic objectives or the other three categories of enterprise risks), it should be tracked and documented on the cybersecurity risk register and included on the cybersecurity risk profile to be reported up to the ERM program as risk inputs. With risk inputs from the cybersecurity risk profile, Enterprise Risk Officers can then consolidate all risk inputs from others to create an enterprise risk register.

As discussed in Sections 3.9 and 4, the Enterprise Risk Register will be prioritized by senior enterprise leaders to create an enterprise risk profile. Prioritizing other types of risks may be done at the discretion of the C-suite or other operating executive staff. Prioritization should include the following considerations:

- How to combine the calculations of likelihood and impact to determine exposure[21],
- How to determine and measure the potential benefits that may accrue from pursuing a particular risk response, and
- When to seek additional guidance on how to evaluate risk exposure levels, such as while evaluating exposures that arise from risks in a focus area.

One example of a quantitative model for rating risk exposure and prioritizing negative and positive risks is the Probability and Impact Matrix illustrated in Figure 5.[22] In the Matrix, each risk is evaluated in light of the risk's likelihood and impact and determined during risk analysis. The thresholds for ranges of exposure can be established and published as part of the enterprise governance model and then used by stakeholders to prioritize each risk in the register.

[21] The formula for calculating risk exposure is the total loss if the risk occurs multiplied by the probability that the risk will happen. Loss is calculated through a traditional Business Impact Analysis (BIA) used in conjunction with the risk register model to inform the senior level decision-making process. See NIST SP 800-34 for additional information.

[22] The Matrix is from NIST SP 800-30, Revision 1, Table I-2 [12].

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Figure 5: Probability and Impact Matrix

Prioritizing risk is a similar process at the system, organization, and enterprise levels. After the exposure for each risk is determined, the risks in the register should be sorted to reflect their priority. The risk priority can be assigned during the cost/benefit analysis (CBA) (see Section 3.5.2). Prioritization can be derived directly from the result of the risk exposure or from a combination of the risk exposure and other factors, such as enterprise context or stakeholder objectives. As the results from each system and organization's risk register are completed, they should be provided to the designated risk officers at the relevant level (i.e., system or organization) and shared with the corporate officers and high-level executives to conduct the following actions:

- Identify and resolve any conflicting risks.
- Correlate common risks among the various systems.
- Normalize definitions and values as recorded by various enterprise entities.
- Aggregate risks in similar categories into a more concise view.

Enterprise Risk Officers collect all risk inputs, including the cybersecurity risk profile from cybersecurity risk officers, and analyze potential risk events, consequences, and impacts at the enterprise level. The aggregated and prioritized Enterprise Risk Register represents a risk profile that enables key executive stakeholders to stay aware of critical risks, including those that are cybersecurity related. For some organizations, this information will need to be provided to Board of Directors-level risk management committees or to other enterprise entities that have a fiduciary duty to remain aware of and help manage risks (discussed in Section 4). In this way, enterprise leaders will have the necessary information and opportunity to consider cybersecurity exposure as factors for budgets or corporate balance sheet reporting.

Just as is the case for private sector entities, this aggregated and prioritized risk register can represent or be part of an enterprise risk profile for federal agencies.[23] The "primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its

[23] Special treatment and communication flow germane to enterprise-level treatment of risk prioritization is discussed in Section 4 of this document.

strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives" [3]. Nonfederal organizations similarly benefit from such prioritization. In fact, one of COSO's key principles includes, "The organization prioritizes risks as a basis for selecting responses to risks" [8]. Given the resources available to an entity, management must evaluate the trade-offs between allocating resources to mitigate one risk compared to another.

As a prioritized inventory of the most significant risks, the risk profile helps consider risks from a portfolio perspective and provides executive leaders with an understanding of sources of uncertainty, both positive (opportunities) and negative (threats). Relevant risks are selected for an evaluation of risk response strategies, as described below.

3.5 Plan and Execute Risk Response Strategies

The fifth step from Figure 2 is to determine the appropriate response to each risk. The goal for effective risk management, including cybersecurity risks, is to identify ways to keep risk aligned with the risk appetite or tolerance in as cost-effective a way as possible. In this stage, the cybersecurity risk officer will determine whether, based on the potential consequences, the exposure associated with each risk in the register is within acceptable levels. If not, that cybersecurity risk officer can identify and select cost-effective risk response options to achieve cybersecurity objectives. The ERM risk officer also coordinates with respective organizations and risk owners to identify and select cost-effective risk response options to achieve their enterprise objectives across the four areas: strategic, operations, reporting, and compliance.

Planning and executing risk responses is an iterative activity and should be based on the risk strategy guidance described in Section 3.1.2. The response selected for each risk will be informed by executives' guidance regarding risk appetite and risk tolerance; as the risk oversight authorities monitor the success of those responses, they will provide financial and mission guidance back to operational leaders to inform future risk management activities. In some cases, risk evaluation may lead to a decision to undertake further analysis to confirm estimates or more closely monitor results (as described in Section 3.6).

While there is some variance among the terms used by various risk management frameworks, in general there are four types of actions available for responding to negative cybersecurity risks: *accept, transfer, mitigate,* and *avoid*. These are explained in Table 3.

1239 **Table 3: Response Types for Negative Cybersecurity Risks**

Type	Description
Accept	Accept cybersecurity risk within risk tolerance levels without the need for additional action.
Transfer	For cybersecurity risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., cybersecurity insurance). While some of the financial consequences may be transferrable, there are often consequences that cannot be transferred, like loss of customer trust.
Mitigate	Apply actions (e.g., security controls discussed in Section 3.5.1) that reduce the threats, vulnerabilities, and impacts of a given risk to an acceptable level. Responses could include those that help prevent a loss (i.e., reducing the probability of occurrence or the likelihood that a threat event materializes/succeeds) or that help limit such a loss by decreasing the amount of damage and liability.
Avoid	Apply responses to ensure that the risk does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing the cybersecurity risk to an acceptable level. The cost of the lost opportunity associated with such a decision should be considered as well.

1240 Risk response will often involve creating a *risk reserve* to avoid or mitigate an identified
1241 negative risk or to realize or enhance an identified positive risk. A risk reserve is similar to other
1242 types of management reserves in that funding or labor hours are set aside and employed if a risk
1243 is triggered to ensure that the opportunity is realized or that the threat is avoided. For example,
1244 the technical skill of subject matter experts to recover after a cybersecurity attack may not be
1245 available with current staffing resources. A risk reserve can also be used with the *accept*
1246 response type to address this by setting aside funds during project planning to employ a qualified
1247 third party to augment the internal incident response and recovery effort.

1248 ### 3.5.1 Applying Security Controls to Reduce Risk Exposure

1249 In many cases, mitigation to bring exposure to negative cybersecurity risks to within risk
1250 tolerance levels is accomplished using security controls. For example, if the Risk Executive
1251 Function declares that the organization must avoid risks with qualitative likelihood and impact
1252 values of High/High for all costs under $500,000, the Risk Response Type column of the risk
1253 register (see Figure 2) can be updated with a response type from Table 3. The Risk Response
1254 Description column can be populated with the NIST Cybersecurity Framework Subcategory
1255 outcomes and NIST SP 800-53 control descriptions that address negative risks, as illustrated in
1256 Figure 6.

1257 NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and*
1258 *Organizations*, provides a comprehensive catalog of technical and non-technical (i.e.,
1259 administrative) controls that act as "safeguards or countermeasures prescribed for an information
1260 system or an organization to protect the confidentiality, integrity, and availability of the system
1261 and its information." It also describes privacy controls that "are the administrative, technical, and
1262 physical safeguards employed within an agency to ensure compliance with applicable privacy
1263 requirements and to manage privacy risks" [5].

1264 Various types of controls may be applied to achieve an acceptable level of risk:

1265 - **Preventative**: Reduce or eliminate specific instances of a vulnerability
1266 - **Deterrent**: Reduce the likelihood of a threat event by dissuading a threat actor

- **Detective**: Provide warning of a successful or attempted threat event
- **Corrective**: Reduce exposure by offsetting the impact of consequences after a risk event
- **Compensating**: Apply one or more controls to adjust for a weakness in another control

Consider an organization that identifies several high-exposure negative cybersecurity risks,[24] including that poor authentication practices (e.g., weak or reused passwords) could enable the disclosure of sensitive customer financial information and that employees of the software provider might gain unauthorized access and tamper with the financial data. The organization can apply several deterrent controls (documenting the applied control identifiers and any applicable notes in the risk register comments column), including warning banners and the threat of prosecution for any threat actors that intentionally attempt to gain unauthorized access. Preventative controls include applying strong identity management policies and using multi-factor authentication tokens that help reduce authentication vulnerabilities. The software provider has installed detective controls that monitor access logs and alert the organization's security operations center if internal staff connect to the customer database without a need for access. Furthermore, the financial database is encrypted so that it protects its data if the file system is exfiltrated.

To confirm that the intended mitigation techniques are effective (and cost-effective), the application of the controls should be evaluated by a competent assessor. Because this example includes several third-party supply chain partners, that assessment will likely include multiple parties. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, provides detailed criteria for examining the application of controls and processes, testing control effectiveness, and conducting interviews to confirm that the mitigation techniques are likely to achieve their intended result [22].

3.5.2 Responding to Residual Risk

Section 3.2 briefly introduced the concept of residual risk. *Residual risk*, also referred to as post-treated risk, is risk that remains after risk responses (listed in Table 3 and Table 5) have been documented in the cybersecurity risk register and performed against the inherent risk listed in the same row, as depicted in the fictitious example portrayed in Figure 6. The residual risk can be calculated using the same methods for calculating inherent risk discussed in Section 3.3. If the residual risk is outside of the acceptable level of risk, a cost/benefit analysis should be performed. Through this process, the appropriate level of management should make a decision as to when the risk planning process will stop. Residual risks that are deemed acceptable should be clearly communicated to management.

[24] Negative risks are determined in NIST Cybersecurity Framework *Step 6: Determine, Analyze, and Prioritize Gaps*, as described in Section 3.2.2.

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Impact	Likelihood	Exposure Rating					
1	5	External thief steals a PC tower from the reception area.	Physical and Environmental Protection (PE)	.1	.75	7.5% (Low)	Accept	$0	• None required	Kira Caldwell	Open
2	1	External malicious actor deploys a ransomware attack causing unavailability of financial systems	System and Information Integrity (IS)	.9	.9	80% (High)	Mitigate	$3.7 M	• Segment internal networks (AC-4, NIST CSF PR.AC-5) • Improve backup plans (CP-9, NIST CSF PR.IP-4)	Jemima Daugherty Carly Hickman (backup)	Open
3	4	A natural disaster disrupts communications circuits impeding customer access	Contingency Planning (CP)	.3	.4	12% (Low)	Transfer	$125,000	• Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
4	3	Human Resource Management Systems move to a cloud solution provides in-house IT infrastructure savings and improves availability	System and Services Acquisition (SA)	.5	.5	25% (Moderate)	Exploit	$2 M	• Conduct migration to SaaS provider • Confirm system reliability • Decommission HR Minicomputer	Amir Marsh	Open
5	2	Portable workstation containing digital designs is lost (e.g., left on an airplane)	System and Communications Protection (SC)	.7	.8	56% (Moderate)	Mitigate	$275,000	• Implement full-disk encryption of sensitive devices (SC-28, NIST CSF PR.DS-1) • Implement remote tracking and erasure solution (MP-6, NIST CSF PR.DS-1)	Jeffrey Contreras	Updated
Continually Communicate, Learn and Update											

Figure 6: Example Cybersecurity Risk Register

A key factor in achieving effectiveness is using a cost/benefit analysis (CBA). IEC 31010 states that a "cost/benefit analysis weighs the total expected costs of options in monetary terms against their total expected benefits in order to choose the most effective or the most profitable option" [21]. Through this analysis, the cybersecurity risk officer can consider the exposure factor cost (i.e., the likely cost of exposure based on the likelihood and impact of a residual risk, as recorded in the risk register) compared to the potential cost of the risk response for that residual risk. For

example, consider Risk #5 from Figure 6. The risk owner might determine that a potential breach resulting from a misplaced or stolen laptop with sensitive design plans could cost $750,000 in disclosed research and missed opportunities. The labor and software to apply full disk encryption and remote tracking on laptops containing sensitive data would cost $275,000, so the benefit is worth the cost of the countermeasures.

Upon approval of the risk response for each risk description and the determination of one or more accountable risk owners, the risk register is updated to reflect that information. OMB Circular A-123 states, "Residual risk is the exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent assessment." Enterprise Risk Officers document residual risks on the enterprise risk profile and analyze these risks against applicable enterprise risk appetite and tolerance levels set by senior leadership. They then determine if any additional risk response plans or actions are needed. Enterprise Risk Officers must communicate these proposed plans and actions to the enterprise's senior management to make the final decisions and then communicate these decisions timely and appropriately to risk owners at lower levels, such as organization or system levels.

Federal agencies develop *a plan of action and milestones* (POA&M) for each system to document the risk responses being planned for its residual risks (generally residual risk that must be accepted for the current time period). A POA&M "identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones." It also "describes the measures planned to correct deficiencies identified in the controls […] and to address known vulnerabilities or security and privacy risks. The content and structure of plans of action and milestones are informed by the risk management strategy developed as part of the risk executive (function)…." [25] POA&Ms serve as an input to the Cybersecurity Risk Register.

3.5.3 When a Risk Event Passes Without Triggering the Event

Risk responses will often be adjusted as opportunities and threats evolve. The concept is similar to the topic sometimes called the "Cone of Uncertainty" within project management practices in that, over time, additional understanding about an identified risk will come to light. One mitigation technique for these types of risk factors is the use of risk reserves introduced in Section 3.5. If this risk response is selected, it is critical that the risk owners collaborate with the acquisition or procurement teams and budget owners. With appropriate budget planning, risk reserves can be released for other predetermined funding requirements after the risk period has expired.

While many industry-based enterprises can return the unused funds to shareholders or pay down corporate debt, unused reserves are more difficult for government agencies to use without preplanning. Most government procurement cycles are rigidly based on the government fiscal year. Identified opportunities can be planned for in government procurement cycles as "optional" tasking or purchases. For example, unused funds could be used to accelerate the IT refresh cycle

[25] For more information, see NIST SP 800-37, Revision 2 [13].

to address cybersecurity risks (e.g., CPU vulnerabilities that resulted in performance losses when patched). If the current fiscal year only allows for the purchase of half of the required materials, an option can be included at the time of the base contract award for the other half of the materials (but not funded at the time of the based contract award). When the cybersecurity risk officer liberates the risk reserve after the chance of the negative risk occurring has passed, the funding can be used to exercise the already awarded option that lacked the initial funding when the base contract was awarded. Exercising an option in government contracting is trivial (often 30 days or less) when compared to the long lead time for initial contract procurements. See the "Integrate and Align Cybersecurity and Acquisition Processes" section of NIST IR 8170 [4] for more information on preplanning for government agencies.

As described in the NIST Cybersecurity Framework, "since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services" [16]. If an organization used the Cybersecurity Framework to create a list of products or services for addressing identified risks, the risk reserve can be used to acquire these predetermined risk mitigation solutions. Once a product or service is purchased, the Target Profile can also be used to track and address residual cybersecurity risk using the risk register.

3.6 Monitor, Evaluate, and Adjust

Managing cybersecurity risk to support mission and business objectives by protecting the value provided by enterprise information and technology requires continual balancing of the benefits, resources, and risk considerations. As an input to ERM, cybersecurity risk management requires a dynamic and collaborative process to maintain that balance by continually monitoring risk parameters, evaluating their relevance to organizational objectives, and adjusting controls when necessary. The risk register provides a formal communication vehicle for sharing and collaborating on cybersecurity risk activities as an input to ERM decision-makers.

From the initial agreement and understanding of internal/external context to discussion and authorization of risk response, continual dialogue is needed among all relevant stakeholders. While such discussions often occur within a given business unit or subordinate organization, the enterprise will benefit from broader, frequent, and transparent communication regarding risk options, decisions, changes, and adjustments because it will improve the quality of information used in making enterprise-level decisions. The evolving cybersecurity risk registers and profiles provide a formal method of communicating institutional knowledge and decisions regarding cybersecurity risks and their contributions to ERM.

3.6.1 Continuous Risk Monitoring

Because cybersecurity risks and their impacts on other risks frequently change, enterprise risk conditions should be continually monitored to ensure that they remain within acceptable levels. For example, such monitoring could determine when negative cybersecurity risks for a system are approaching the risk tolerance level, triggering a review of the risk that could result in a higher priority for the risk and the implementation of additional risk responses. Risk monitoring benefits from a positive risk-aware culture within the enterprise. Such a culture leads to a

cohesive, team-based approach to monitoring and managing risks. Proactive activities, including the examples listed in Table 4, support that kind of culture.

Table 4: Examples of Proactive Risk Management Activities

Activity Example	Description
Cultural Risk Awareness	Encourage employees to look for cybersecurity risk issues before they become significant.
Risk Response Training	Train employees and partners on enterprise strategy, risk appetite, and selected risk responses.
Risk Management Performance	Discuss the impact of cybersecurity risk on every employee and partner and why the effective management of risks is an important part of everyone's job.
Risk Response Preparedness	Conduct exercises to provide practical and meaningful experience in recognizing, reporting, and responding to cybersecurity risk scenarios.
Risk Management Governance	Remind staff of organizational policies and procedures that are established to help improve risk awareness and response.
Risk Transparency	Enable an environment where employees and partners may openly and proactively report potential risk situations without fear of reprisal.

Each risk in the register is assigned a risk owner, as described in Table 2. The risk owner is accountable for applying the priority described in Section 3.4 to select and apply appropriate risk responses while considering business objectives and performance targets. ERM leadership (e.g., the Risk Executive function described in the RMF) should ensure that accountability. ERM programs, policies, and processes should specify the frequency and methods for monitoring, evaluating the effectiveness of, and adjusting risk responses. They should also define the approved governance bodies to discuss, approve, and communicate the most significant risks and their plans.

An element of risk monitoring is determining and publishing accountable risk management roles throughout the enterprise, including those in organizations. The relationships among these entities should be communicated clearly, such as how a formal enterprise risk committee may be informed by subordinate risk councils or working groups. They can help ensure cross-communication among other groups that support risk management, such as human resources, legal, auditing, and compliance management. As one of the primary compliance indicators, OMB Circular A-123 requires federal agencies to consider their management responsibilities for "the establishment of a government structure to effectively implement, direct and oversee implementation of the Circular and all the provisions of a robust process of risk management and internal control." These governance structures formalize the relationships across all levels and operating units within the federal agency.

If the risk response for a given risk (or set of risks) requires a funding or schedule consideration, specific monitoring and measurement milestones can be included in the associated risk response plan. The risk owner can then identify performance measures or trends (e.g., deliverable artifacts or software development achievements) that represent milestones in addressing the risk. Having achieved those milestones may trigger the release or repurposing of the associated management reserve resources. This process can be especially helpful in enterprises that manage funding by periodic increments, such as fiscal years. In such an enterprise, it can be beneficial for the

monitoring process to identify that a given risk is unlikely to occur, allowing the risk owner sufficient time to reallocate those reserves before other funding deadlines.

Based on an ongoing review of cost/benefit analysis, the enterprise should continually monitor the risk register, including those entries that may have been deferred or declined in the past. By continually refreshing the risk register and risk profile artifacts described in this report, this monitoring and adjustment will be straightforward. It is important to communicate and benefit from the lessons learned from previous practice and actual risk events. By examining adverse events and losses from the past and reviewing missed opportunities (including those missed due to a risk-averse mindset), the enterprise can improve the risk management model and organizational outcomes.

Many organizations employ automated processes and software to support continuous risk monitoring. NIST and its National Cybersecurity Center of Excellence (NCCoE) have developed extensive guidance regarding the technical mechanisms available to perform and assess Information Security Continuous Monitoring (ISCM). For ISCM to provide meaningful input into ERM processes, the ISCM must be designed and operated in light of the ERM strategy described above. In this way, the risk dashboard and associated reports provide a visual representation of the information in the risk register. Examples of systems that use such a dashboard include the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) system and the Department of Defense (DoD) Enterprise Mission Assurance Support Service (eMASS).

3.6.2 Key Risk Indicators

One method for improving monitoring is the use of risk indicators. These indicators provide measures that help gauge the probability that a given risk will occur and whether it is likely to exceed the risk appetite. Senior leaders in the enterprise determine appropriate risk indicators based on the internal and external context described above.

Executives may select a subset of those indicators that are especially suitable for predicting or indicating important risk to be Key Risk Indicators (KRIs). These KRIs should be defined in reference to the given risk exposures that have been identified above. Executives should ensure that risk appetite statements focus on ensuring mission and objective success. For example, if a federal agency has a strategic objective to ensure the protection of user data, the agency's risk appetite statement specifies a low tolerance for data breach/disclosure. The agency can deploy an audit control to determine if a breach occurred; however, this control is backward looking and does not plan to thwart the attack. The agency should employ KRIs to detect a data breach before its occurrence, such as participating in information sharing forums to discover common attacks occurring at other agencies or private businesses.[26] Other indicators might be to data-mine packet captured data for information that might indicate an adversary is preparing to move its payload into the enterprise to exfiltrate data. Similarly, an organization might assess download times, network traffic surges, account auditing, statistical deviations from normal user behavior, etc.

[26] See NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* for more information. https://doi.org/10.6028/NIST.SP.800-61r2

This second set of indicators is actionable whereas the audit control is not.

Cybersecurity KRIs can be *positive*, such as the number of critical business systems that include strong authentication protections. They also can be *negative*, such as the number of severe customer disruptions in the last 90 days. Additional measures may include compliance measures, performance targets for positive risk, and objectives for balancing risk and reward. KRIs can also be supplemented by Key Performance Indicators (KPIs) that measure how well a particular process is enabling the achievement of a goal, such as a risk response procedure.

Based on the monitoring and reporting of risk measures, the enterprise and subordinate levels need to identify and provide processes for reassessing risk. Changes in the risk landscape, including those from modifications in industry regulation, may require a periodic review of risk appetite, tolerance, and capacity.

Some of the same types of quantitative and qualitative methods described above may be helpful in conducting such analyses. For example, quantitative KRIs might track customer downtime and could support a root-cause analysis of trends to avoid fines from a missed customer service-level agreement. Similarly, monitoring the successful implementation of a data loss prevention tool could quantify sensitive messages that had been quarantined with a successful mitigation of financial and reputational losses. These observations help identify where processes could have been improved or errors might have been avoided, supporting opportunities for training and updating procedures.

3.6.3 Continuous Improvement

A risk-aware culture should be looking for opportunities for improvement—reinforcing effective practices and adjusting to correct deficiencies. While all should be responsible and held accountable for any negligent activity, there is value in fostering a community that pursues opportunities within risk appetite levels while also being prepared for and continually thwarting threat actors that would exploit vulnerabilities.

The Plan-Do-Check-Act approach is a well-known model for achieving ongoing effectiveness of any process, and it applies well to cybersecurity risk management. Earlier in Section 3, this report described methods for the Plan and Do elements—essentially, planning based on enterprise direction and carrying out activities to achieve an acceptable level of cybersecurity risk. Section 3.6.1 describes the Check element, where the cybersecurity risk officer determines whether the intended activities accomplished objectives and to what extent. The remaining element, Act, helps determine what should be done next to adjust and improve.

An element of adjustment relates to learning from open and transparent feedback throughout ERM communications processes. Figure 2 points out that communication takes place throughout the risk management life cycle—including risk direction, identification of threats and opportunities, analysis of resulting exposure, and implementation of responses—and that the risk register is the vehicle for all of those communications. Each of these activities provides a chance for feedback and documenting lessons learned to drive subsequent improvement. By staying aware of changes to the risk landscape—such as through subscriptions to community alerts (e.g.,

InfraGard, US-CERT, commercial threat feeds), industry and public-sector workshops, and publications (e.g., NIST publications and postings)—cybersecurity risk officers can adjust risk identification and assessment processes for emerging and evolving threats and opportunities.

As risk register and profile information is collected and aggregated (described in detail in Section 4), leaders can provide feedback to improve processes and adjust risk criteria. Perhaps a new online service offering provides an opportunity to innovate, so leadership has directed the organization to take a little more risk and potentially improve revenues. Alternatively, perhaps other business units have suffered some cybersecurity attacks, and stakeholders have reevaluated the likelihood and impact criteria. In either case, the ability to adjust the effective management of cybersecurity risk supports broad enterprise objectives as part of ERM.

3.7 Considerations of Positive Risks as an Input to ERM

Planning for success is equally as important as avoiding disasters. As mentioned in Section 3.2.2, OMB states in Circular A-123 that regarding the inclusion of opportunities (positive risks) as a function of the ERM profile, "the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)."

In the discipline of cybersecurity risk management, a significant portion of risk information is collected and reported with regard to weaknesses and threats that could result in negative consequences. However, positive risks (opportunities) also support decisions by those executives for setting the risk appetite and tolerance of the enterprise. For example, conducting a SWOT Analysis that considers strengths *and* weaknesses as well as threats *and* opportunities may be a useful exercise.

Consider, for example, an organization that is evaluating moving a major financial system from an in-house data center to a commercial hosting provider. If the organization maintains vast amounts of land and warehouses, this could be considered a strength of the organization, and they might increase revenue by offering space to a commercial vendor to host both their own and other organizations' data centers. The Federal Government has realized many opportunities of this nature, including consolidating payroll functions under the National Finance Center (NFC) and consolidating reporting requirements in the Department of Justice Cyber Security Assessment and Management (CSAM) application.

Section 3.2.2 describes the need to treat threat actors and threat sources as inputs into an estimation of risk. If the enterprise chooses to include positive risk scenarios in the register, then the process should similarly consider *sources of opportunity* that might provide benefits. A consideration of both threats and opportunities may enable discussions regarding the benefits and risks of a particular endeavor. Alternatively, the organization could manage an *opportunity risk register* separately from the traditional threat-based risk register since positive risks (i.e., opportunities) often have to be assessed on a slightly different scale.

In addition to the threat modeling examples above, methods for identifying cybersecurity-specific opportunities are also available and could be as simple as an employee suggestion box. Industry publications, such as those from commercial industry associations and agencies like

NIST, regularly provide information and ideas regarding potential innovations or advances that may represent cybersecurity opportunities.

Numerous formal methods are available for identifying opportunities, including:

- **Brainstorming** – A group innovation technique, often led by a facilitator, that elicits views from participants to identify and describe opportunities
- **Delphi** – A procedure to gain consensus from a group of subject matter experts using one or more individual questionnaires that are then collected and collated to identify opportunities to be pursued
- **Ideation** – A consistent process of observing an environment, discerning opportunities for improvement, experimenting with possible resolutions, and developing innovative solutions

The same formal methods can be used for determining other inputs, such as those described in Section 3.2.3 and Section 3.2.4.

With regard to positive risk response, consider the previous example of an organization that has identified the positive risk of increasing revenue by providing physical space for a commercial vendor to provide an outsourcing service. Analysis of the risk has determined that the opportunity would be highly beneficial to the enterprise. The solution also provides a moderate opportunity to improve availability because of the colocation. The Risk Response Type column of the risk register should also be updated using a response type from Table 5, the comment field updated to contain information pertinent to the opportunity, and the residual risk uncertainty of not realizing the opportunity calculated as discussed in Section 3.5.2.

With these controls and methods in place and assessed as effective, the remaining risks can be analyzed as described in Section 3.3 to determine the residual impact, likelihood, and exposure. If the residual exposure falls within risk tolerance levels, then stakeholders can proceed in gaining the benefits of the opportunity. Each of these values is added to the risk register for enterprise reporting and monitoring.

Where positive risks are to be considered and included in risk registers, there are four generally used response types for positive cybersecurity risks, as explained in Table 5.

Table 5: Response Types for Positive Cybersecurity Risks

Type	Description
Realize	Eliminate uncertainty to make sure the opportunity is taken advantage of.
Share	Allocate ownership to another party that is better able to capture the opportunity.
Enhance	Increase the probability and positive impact of an opportunity (e.g., invest in or participate with a promising cybersecurity technology).
Accept	Take advantage of an opportunity if it happens to present itself (e.g., hire key staff, embrace new cybersecurity technology).

As with negative risks, positive entries in the cybersecurity risk registers may be normalized and aggregated into the enterprise-level risk register.

3.8 Creating and Maintaining an Enterprise-Level Risk Register

A key outcome of the risk identification and communications elements is the ability to create an enterprise risk register. As described at the beginning of this section, the application of a consistent risk register with agreed-upon criteria and categories enables various data points to be normalized, aggregated, and sorted into an enterprise-wide view. While this report illustrates it as a table, many organizations maintain a formal application that provides that tracking and reporting (e.g., a GRC product.)

As part of the risk guidance, enterprise leaders will designate the ERM process participants and the responsibilities of each role. That guidance should declare the role responsible for creating and maintaining the Enterprise Risk Register, the frequency with which that will be updated, and how the risks within the register will be communicated to various stakeholders. This report will consider that role to be assigned to the Enterprise Risk Officer, although the responsibility could fall upon any designated party, including other roles as described in Section 3.1.1.

The creation and maintenance of the Enterprise Risk Register also supports a periodic review of the enterprise risk guidance, including risk definitions, context, and risk appetite criteria. It provides an opportunity to review and validate enterprise definitions for risks, risk categories, and risk assessment scales. If any changes or updates to the risk context or guidance need to occur, the enterprise Risk Officer (or equivalent) is likely to have sufficient seniority to ensure appropriate updates to those enterprise processes.

3.9 Cybersecurity Risk Data Conditioned for Enterprise Risk Rollup

To support the subsequent aggregation of various risk registers, enterprise risk guidance should identify the enterprise objectives to which various types of cybersecurity risk should be aligned. Section 4 of this report describes an Enterprise Risk Profile that reflects risks that may impact the enterprise in each of four discrete objectives: strategic, operations, reporting, and compliance. These same four objectives were key factors in the original COSO ERM framework and are often used as guideposts for enterprise risk reporting. Clear direction from senior executives about how to align various types of cybersecurity risk with enterprise objectives will help enable subsequent aggregation, normalization, and prioritization.

Example alignments might include:

- **Strategic**: risks related to the implementation of a new service offering; cybersecurity issues that might impact an upcoming federal agency merger or private sector acquisition
- **Operations**: cybersecurity issues regarding existing operational systems, such as a ransomware attack that disables a manufacturing line; business continuity/disaster recovery issues
- **Reporting**: cybersecurity risks regarding the availability, integrity, and confidentiality of accounting or other financial management systems
- **Compliance**: cybersecurity risks where a negative event might result in a failure to meet a contractual service agreement or in a regulatory penalty or fine

If the Cybersecurity Risk Register employed NIST SP 800-53 families as its organizing principle for categories, a predetermined mapping between the family and one of the four Enterprise objectives could streamline the cybersecurity risk to enterprise risk rollup process. Direction may be needed regarding how to account for those risks that cross multiple boundaries and how each organizational level should perform an aggregation of subordinate risk registers.

Table 6 provides a notional enterprise risk register that combines both federal agency and critical infrastructure risks, illustrating the integration of various cybersecurity risks alongside other key enterprise risks.

Table 6: Notional Enterprise Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment					Risk Response	Risk Owner	Status
				Financial Impact	Reputation Impact	Mission Impact	Likelihood	Exposure Rating			
1	5	Retiring staff lead to personnel shortages	Operational Risk	OpEx M CapEx L	L	M	M	M	• Improve hiring diversity • Improve employee benefits packages per recent survey and discussions	Human Resources Department	Open
2	6	A strategic opportunity to hire a globally recognized technologist leads to establishing a new satellite communications initiative[27]	Operational Risk	OpEx M CapEx L	H	M	M	M	• Allocate funds for compensation package • Initiate strategic recruiting plan	Human Resources Department	Open
3	1	A social engineering attack on enterprise workforce leads to a breach or loss	Operational Risk	OpEx M CapEx L	H	M	H	H	• Update corporate IT security training • Implement phishing training service • Update email security products per recommendations from IT Risk Council	CISO	Open
4	3	A security event at a third-party partner results in data loss or system outage	Operational Risk	OpEx L CapEx L	H	H	M	M	• Chief Financial Officer and Chief Executive Officer to agree on plans for likely secondary financial impact from the high-rated reputational risk impact • Update procurement contract requirements to include protection, detection, and notification clauses per 11/3/2019 report from Legal Dept • Implement 3rd Party Partner Assessment for Tier 1 providers per CIO & CISO recommendations	Procurement	Open

[27] Example treatment of an opportunity (positive risk).

ID	Priority	Risk Description	Risk Category	Current Assessment					Risk Response	Risk Owner	Status
				Financial Impact	Reputation Impact	Mission Impact	Likelihood	Exposure Rating			
5	7	Sales reduction due to tariffs leads to reduced revenues	Financial Risk	OpEx M CapEx L	L	L	L	L	• Increase marketing in target areas • Ensure competitive pricing in target markets	VP Sales	Open
6	8	Customer budget tightening results in reduced revenue and profits	Financial Risk	OpEx M CapEx L	L	L	M	M	• Implement customer surveys to better forecast potential changes in purchasing patterns • Improve cost-cutting measures to offset reductions and maintain profitability	VP Sales	Open
7	9	Failure to innovate results in market share erosion	Strategic Risk	OpEx M CapEx M	M	L	M	L	• Approve CIO proposal to increase Internal Research & Development (IRAD) funding by 10% to spur and expand internal innovation • Update technical training to include design thinking methodologies • Implement customer surveys in target areas to ensure adequate product coverage	VP, Product Development	Open
8	2	Company intellectual property data is disclosed through employee error or malicious act	Operational Risk	OpEx M CapEx M	H	H	M	M	• Review employee background screening controls and improve, if necessary • Update corporate security training to reinforce the need for diligence • Implement data loss prevention tools per CISO recommendation	CISO	Closed
9	10	A flaw in product quality leads to reputational damage, reducing sales	Strategic Risk	OpEx M CapEx M	H	H	L	L	• Update continuous improvement process • Implement Baldrige Excellence Framework • Update external provider quality standards	VP, Product Development	Open
10	4	A regulatory compliance failure exposes the company to fines, penalties, and legal fees	Compliance Risk	OpEx M CapEx L	H	L	M	M	• Create & maintain a centralized register of compliance requirements • Update employee training based on an updated understanding of corporate requirements • Review business impact assessment (BIA) templates to ensure that information and technology requirements include regulatory and contractual obligation criteria	Legal Dept.	Open

1609

Table 7 describes each of the elements in the example Enterprise Risk Register.

Table 7: Descriptions of the Notional Enterprise Risk Register Elements

Register Element	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register (e.g., 1, 2, 3)
Priority	A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low). Note that this prioritization may differ from similar risks in individual risk profiles from subordinate organizations.
Risk Description	A brief explanation of the cybersecurity risk scenario impacting the enterprise
Risk Category	An organizing construct that helps to evaluate similar types of risk at the enterprise level. Categories also help with consolidation and normalization of information from subordinate risk registers. Organizations draw from many available taxonomies of risk categories; these examples use the taxonomy described in the US Government Federal ERM Playbook [2].
Current Assessment—Financial Impact	Analysis of the financial potential benefits or consequences resulting from this scenario. While this element could be quantitative, it is often qualitative (e.g., high, moderate, low) at the enterprise level. Financial considerations may be expressed as (1) capital expenditures (CapEx) that represent a longer-term business expense, such as property, facilities, or equipment, and (2) operating expenses (OpEx) that support day-to-day operations.
Current Assessment—Reputation Impact	Analysis of the potential benefits or consequences that the scenario might have on the stature, credibility, or effectiveness of the enterprise. Some enterprises perform a formal sentiment analysis using commercial services or other technical tools to support assessment.
Current Assessment—Mission Impact	Analysis of the potential benefits or consequences that the scenario might have on the ability of the enterprise to successfully achieve mission objectives
Current Assessment—Likelihood	An estimation of the probability, before any risk response, that this scenario will occur. This considers the effectiveness of current key controls.
Current Assessment—Exposure Rating	A calculation of the likely risk exposure based on the inherent likelihood estimate of probability and the determined mission, financial, and reputational benefits or consequences of the risk
Risk Response	A brief prose description of the selected risk response strategy
Risk Owner	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The Risk Owner may work with a designated Risk Manager who is responsible for managing and monitoring the selected risk response.
Status	A field for tracking the current condition of this risk and any next steps

As was described for cybersecurity risk registers, there is value in both a single point of reference (the register) and detailed risk information (the risk detail report). The risk register provides an easily consumed summary for understanding the risk landscape, while the detailed version provides additional information. The risk detail report also enables additional information, such as historical information, detailed risk analysis data, and information about individual and organizational accountability.

Additional information for inclusion in an Enterprise Risk Detail Report might include:

- Detailed risk information (e.g., full risk statement, detailed scenario description, key risk indicators, enterprise status for this particular risk)

- Information regarding various risk roles (e.g., Risk Owner, Risk Manager, Risk Approver, if applicable) and affected stakeholders
- Historical timeline information (e.g., last update date, next expected review)
- Risk analysis information, including the aggregate understanding of threats, vulnerabilities, resources affected, and impact
- Detailed risk response information (e.g., responses implemented, status and results of previous responses, additional responses planned)

The Enterprise Risk Register provides an input for those performing enterprise risk oversight, such as an executive risk committee. The register acts as an informative gauge that can be used to stay aware of various risks, including those related to cybersecurity. By tracking the status of each risk, including the exposure value of each, enterprise stakeholders can identify the most relevant risks (e.g., a top ten list that may be used to further inform enterprise risk decisions). Summary reports about the highest priority risks may be used to inform stakeholders (e.g., those in an oversight role such as Congress, OMB, or Government Accountability Office [GAO]) about existing risks, risk responses, and planned activities.

Since it is difficult to compare dissimilar risk exposures, such as employee retention and disaster recovery, risks are often translated into financial impact and may be further decomposed into direct cost (i.e., the impact of a given risk on the capital budget and operating expenses), the financial cost of reputational damage, and direct financial implications of impact on the enterprise mission. The relative financial impact of each type of risk can provide further input into risk management prioritization and monitoring decisions for enterprise risk managers. Reputation exposure can be similarly determined in the Enterprise Risk Register (e.g., by the CRO) by combining high-impact attacks, enterprise sector, and consequences with a histograms (trend) analysis of stakeholder sentiment (for each stakeholder type). This last step of prioritization creates the Enterprise Risk Profile, as discussed in Section 4.

4 Cybersecurity Risk Management as Part of a Portfolio View

The objective of ERM deliberations and related decisions is to provide timely resource allocation and mission guidance to enterprises and to prepare prudent risk position disclosures to appropriate stakeholders. OMB Circular A-123 recommends a portfolio view of risk that "provides insight into all areas of organizational exposure to risk […] thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment" [3]. This portfolio view is valuable to all enterprises, public and private. While many ERM processes are written from a commercial perspective, agency "enterprises" operate differently but experience similar financial and reputation risk impacts. In fact, the federal budget presents the same income, capital, and cash flow statements as public companies. Likewise, federal ERM best practices and guidelines are like those of commercial practices.

For example, U.S. publicly traded companies will typically disclose Information Security in Section 1.A. Risk Factors of Form 10-Q/K filings with the SEC. At this level of reporting, Information Security would be considered an Enterprise Risk Statement. Information Security can be dissected into intermediate risk statements, such as Electronic Information Security and Physical Information Security. Each of these intermediate risk statements can be further broken down into individual risk register statements as detail is required.

To make resource and guidance decisions commensurate with enterprise risk, ERM officials require subordinate organizations' risk registers and profiles to be normalized and aggregated into an enterprise risk register. Those ERM officials then prioritize the risks on the Enterprise Risk Register in the context of achieving the set enterprise objectives—strategic, operations, reporting, and compliance—to develop an Enterprise Risk Profile (described in Section 4.1). NIST often references a strategic view at the enterprise level, supported by business units that implement that strategy and are in turn supported by information and systems that enable tactical implementation of the enterprise objectives. That view is illustrated by the Information and Decision Flows diagram from the NIST Cybersecurity Framework [15] shown in Figure 7.[28]

It is important to remember that these cybersecurity risk inputs are not intended to address all risks that may affect the enterprise objectives. However, considering these risks in light of those objectives enables a proactive and mission-oriented view and supports decisions by enterprise leadership. The intent of normalizing and aggregating the risk register is not to simply create a list of risks in a vacuum. Instead, this enterprise risk register view provides a way to inform enterprise risk managers about the portfolio view of various risks throughout the enterprise, and it supports a holistic understanding of risk treatment.

[28] Adopting and using cybersecurity risk registers is the quickest way for an enterprise to progress from Cybersecurity Framework Tier 1: Partial to Tier 4: Adaptive.

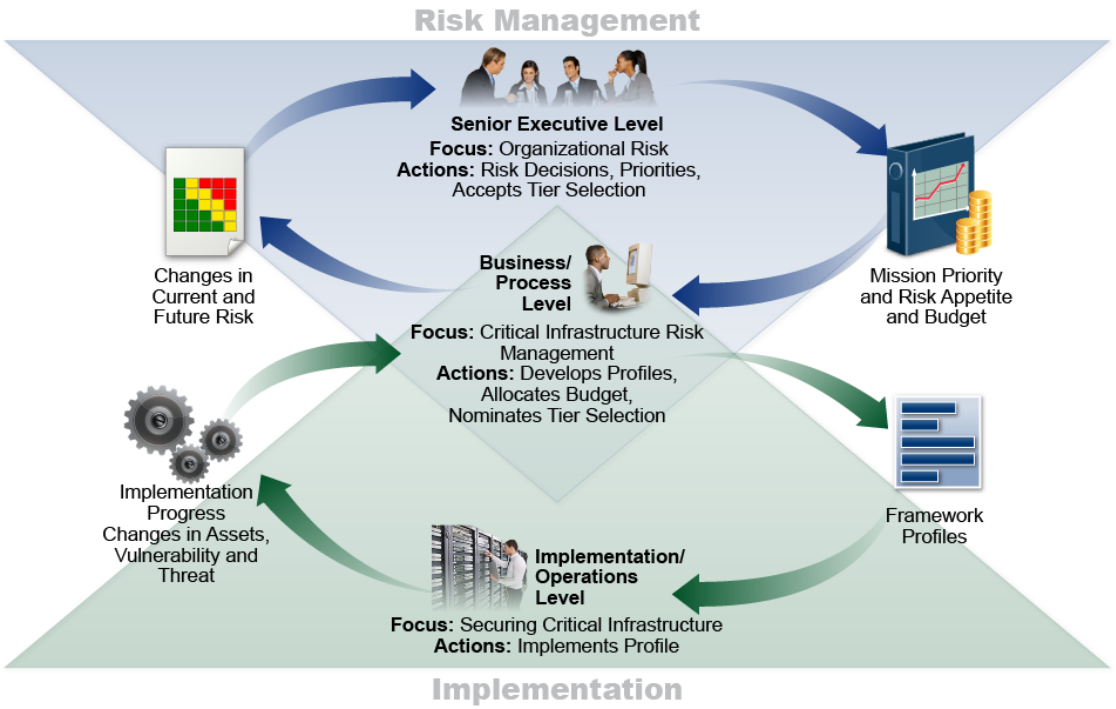


Figure 7: Notional Information and Decision Flows Diagram from NIST Cybersecurity Framework

4.1 Applying the Enterprise Risk Register and Developing the Enterprise Risk Profile

As risk information is transmitted from lower tiers of the organization up to higher tiers, each tier's risk register contains the pertinent information to create a prioritized risk profile for the tier immediately above it. Subordinate organizations' impacts may be different, similar, conflicting, overlapping, or unavailable and must be properly combined by financial and mission analysis at the tier immediately above the reporting organization. While the impacts of cybersecurity risk on various assets may be determined at lower levels, the overall cash flow and capital implications of all of the risks can only be normalized and aggregated (and recorded in the Enterprise Risk Register) by enterprise fiduciaries (e.g., CFOs). Similarly, enterprise mission impacts must be aggregated and expressed by those senior executives most directly accountable to stakeholders.

The Enterprise Risk Register informs the Enterprise Risk Profile once the risks are prioritized at the highest level of the Risk Management Function in the enterprise, as depicted in Figure 8. The Enterprise Risk Profile is a subset of carefully selected risks from the larger Enterprise Risk Register. Although they are maintained as separate documents, though inextricably linked.

STRATEGIC OBJECTIVE – Improve Program Outcomes								
	Current Assessment		Current Risk Response	Residual Assessment		Proposed Risk Response	Owner	Proposed Risk Response Category
Risk	Impact	Likelihood		Impact	Likelihood			
Agency X may fail to achieve program targets due to a lack of capacity at program partners.	High	High	REDUCTION: Agency X has developed a program to provide program partners with technical assistance.	High	Medium	Agency X will monitor the capacity of program partners through quarterly reporting from partners.	Primary – Program Office	Primary – Strategic Review
OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations								
Contract and Grant fraud.	High	Medium	REDUCTION: Agency X has developed procedures to ensure that contract performance is monitored and proper checks and balances are in place.	High	Medium	Agency X will provide training on fraud awareness, identification, prevention, and reporting.	Primary – Contract-ing or Grants Officer	Primary – Internal Control Assessment
REPORTING OBJECTIVE – Provide Reliable External Financial Reporting								
	Current Assessment		Risk Response	Residual Assessment		Proposed Action	Owner	Proposed Action Category
RISK	Impact	Likelihood		Impact	Likelihood			
Agency X identified material weaknesses in internal control.	High	High	REDUCTION: Agency X has developed corrective actions to provide program partners with technical assistance.	High	Medium	Agency X will monitor corrective actions in consultation with OMB to maintain audit opinion.	Primary – Chief Financial Officer	Primary – Internal Control Assessment
COMPLIANCE OBJECTIVE – Comply with the Improper Payments Legislation								
Program X is highly susceptible to significant improper payments.	High	High	REDUCTION: Agency X has developed corrective actions to that ensure improper payment rates are monitored and reduced.	High	Medium	Agency X will develop budget proposals to strengthen program integrity.	Primary – Program Office	Primary – Internal Control Assessment and Strategic Review

Figure 8: Illustrative Example of a Risk Profile (OMB A-123)

The Enterprise Risk Profile reflects assessments of mission, financial, and reputation exposures organized according to the four enterprise objectives. They may be full-value exposures or modified (and so noted) by the likelihood assessments of enterprise executives. At the top

enterprise tier, ERM officials have the prerogative to add their own judgment of likelihood and impact as part of the normalization process, along with other members of the Enterprise Risk Executive function. While the ERM process helps drive the discussion and calculation of likely risk scenarios, recent natural disasters have demonstrated that actual consequences can far exceed initial loss expectations. Enterprise executives should continually observe industry trends and actual occurrences to readjust likelihood and impact estimations and reserves based on a changing risk landscape. Enterprise Risk Profiles should also reflect comparable occurrence incidents and trends for the subject enterprise and peer organizations.

The Enterprise Risk Profile supports the governance and management of risk in several ways:

- **Financial Impact** – Various risk scenarios are converted into actual capital and operational expenses, enabling executive leaders to conduct a fiscally responsible cost/benefit analysis that considers the recommended strategies for risk response. (These presentations are equivalent to the financial disclosures in Form 10-Q and Form 10-K filings to the U.S. Securities and Exchange Commission [SEC] by commercial public companies each quarter and for Form 8-K filings as risk incidents occur.)
- **Reputation Impact** – While subordinate risk registers describe risk scenarios, including those that may impact reputation, executive leaders record the evaluation of consequences on the *enterprise's* reputation. This also supports consideration of other downstream impacts, such as financial losses or credit risk, that are likely to result from damage to reputation.
- **Mission Impact** – Executive leaders record the evaluation of consequences on the overall ability for the enterprise to conduct its mission and achieve strategic objectives. (Mission impact in commercial public enterprises is often expressed in Share Value/Market Cap and Share Volatility tables, also disclosed in SEC filings and shareholder communications.)

These three high-level impact considerations are then used in conjunction with other enterprise risk responses to determine tolerances, allocations, and disclosures commensurate with risk exposure.

4.2 Translating the Risk Profile to Inform Boardroom Decisions

The qualitative data presented in Figure 8 must be distilled into actionable information for executive decision-making during boardroom deliberations. Table 8 provides a notional Enterprise Risk Profile Supplement that reflects a portfolio evaluation of various organizational risk profiles. This information, having been populated and prioritized, directly informs their decision-making responsibilities.

1745 **Table 8: Notional Enterprise Risk Portfolio View for a Private Corporation**

Financial Risk Profile						
	Current Period			**Previous Period**		
	Net Revenue	Capital	Free Cash Flow	Net Revenue	Capital	Free Cash Flow
Enterprise						
Dept A						
Dept B						
…						
Dept N						
Reputation Risk Profile						
	Current Period			**Previous Period**		
	Public	Regulators	Partners	Public	Regulators	Partners
Enterprise						
Dept A						
Dept B						
…						
Dept N						
Mission Risk Profile				**Previous Period**		
Enterprise						
Dept A						
Dept B						
…						
Dept N						

1746 4.3 Information and Decision Flows in Support of ERM

1747 As stated in Section 2.1, senior enterprise executives provide risk guidance—including advice
1748 regarding mission priority, risk appetite and tolerance guidance, and capital and operating
1749 expenses to manage known risks—to the organizations within their purview. Based on those
1750 governance structures, organization managers achieve their business objectives by managing and
1751 monitoring processes that properly balance the risks and resource utilization with the value
1752 created by information and technology. The left side of Figure 9 represents important
1753 information flow in support of ERM. Prioritized risk profile information is developed at each
1754 level and also normalized and summarized for enterprise consideration. Through reports of
1755 successes, challenges, opportunities, and increased risk, as reflected in risk registers, enterprise-
1756 level managers can manage, monitor, and report potential implications to (and from) the risk
1757 profile with a portfolio perspective.

Enterprise-focused activities do not relieve risk owners of their responsibilities within their own organizations. While the phrase "think globally, act locally" was not coined to support cybersecurity risk, the notion applies. Individual cybersecurity risks are managed and tracked within each organization and will likely be handled differently in each. Each organization's risk officer develops its assessment of risks (through the risk profile) relative to its business objectives and risk tolerance. Enterprise risk officers then consider the overall set of risks to determine how the composite set compares to the overall risk appetite. Those enterprise risk officers might maintain the current course of action or take additional steps to reduce risk. They might determine that the overall risk is significantly less than the enterprise risk appetite and decide to motivate organizational risk officers to accept greater risk in targeted areas in order to enhance that organization's value.

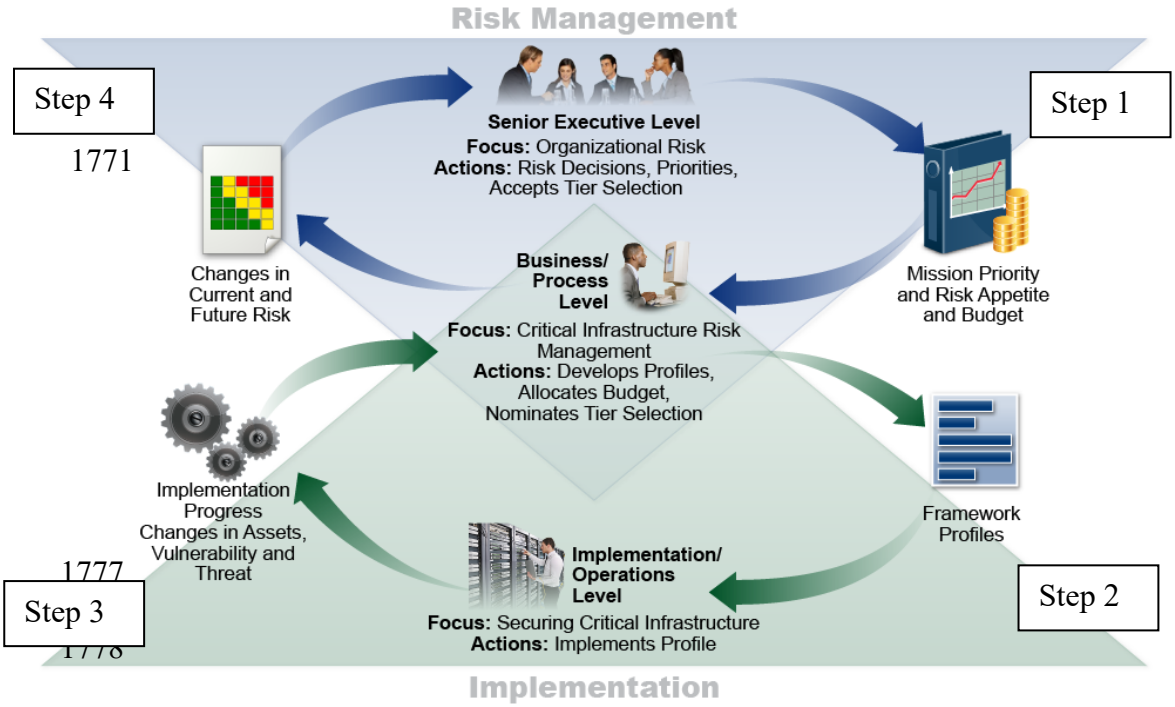


Figure 9: Notional Information and Decision Flows Diagram with Steps Numbered

The following process considers the information and decision flows depicted in Figure 9.

- **Step 1, ERM Result** involves risk direction. Senior executive leaders (e.g., public officials, such as department secretaries or agency directors, and immediate subordinate executives, corporate boards, and their executive fiduciaries) consider the relative importance of various environmental factors. External factors may include political, economic, social, technological, legal, and environmental considerations; internal factors may include the enterprise's capital assets, people, processes, and technology. These leaders may determine how those factors contribute to potential exposure, such as achieving its mission, improving operations, enhancing reporting reliability, and compliance postures. With the factors in mind, senior executive leaders determine risk acceptance levels and resource allocations for all risk types commensurate with impact and likelihood and balanced among and between all enterprise risk exposures.

The result is mission and financial guidance for operational leaders at the business/process level, including direction regarding available budget ceilings for cybersecurity CapEx and OpEx and objectives for free cash flow. Direction regarding risk appetite will vary by enterprise. As with risk analysis, risk appetite may be communicated using qualitative, quantitative, and semi-qualitative methods. It could be expressed as "low appetite" or "high appetite" for various risk categories or expressed numerically, such as through a target percentage, a range of permissible downtime or financial losses, or a ceiling (e.g., up to $1,000,000 in expenses).

- In **step 2, Cybersecurity Activity 1**, organizational managers receive this guidance and perform similar analysis for any subordinate organizations. They then conduct cybersecurity risk management activities as described in Section 3. One process that these managers may apply is the NIST Cybersecurity Framework itself [15]. Based on five Functions—Identify, Protect, Detect, Respond, and Recover—that organize basic cybersecurity activities, that model can assist managers with framing, assessing, managing, responding to, and reporting risks within the business unit and in support of enterprise objectives. The organization can use one or more Target State Profiles (the organizing principles for control selection) that express desired cybersecurity risk management outcomes. Implementation and operation staff then apply those principles to their systems through the RMF or other mechanisms [13].
- In **step 3, Cybersecurity Activity 2**, as risk is managed at the system level in accordance with organizational direction, risk acceptance and monitoring results are provided to the organization stakeholders. The risk determinations, decisions, and status are reported through the organizational risk register and adjusted as necessary (see Section 3.6).
- In **step 4, Cybersecurity Resulting Translation to ERM**, high-level executives without fiduciary reporting requirements (organization) and corporate officers with fiduciary reporting requirements (enterprise) respectively act upon risk registers, aggregating the information, normalizing results, and informing decisions. The risk categories facilitate normalization and reporting. Through this process of collating, aggregating, normalizing, and deconflicting risk register information, the Enterprise Risk Officers and risk committees can:
  - Report understanding of actual and potential risks from threats and system failures to enterprise information and technology.
  - Normalize risk management across the enterprise. For example, if different exposure scales were used in two business units, a "high risk exposure" in one may represent a "moderate risk exposure" under the same conditions in another. Organizations may consider using the same enterprise-level risk lexicon and criteria for consistent messaging as they report risks upwards through the enterprise.
  - Provide enterprise executives with information to measure and understand potential exposure on achieving four enterprise objectives: strategic, operations, reporting, and compliance.
  - Inform operational risk mitigation activities and relate these to enterprise mission and budgetary guidance to prioritize and implement appropriate responses.

- Produce enterprise-level risk disclosures for required filings and hearings or for formal reports as required (e.g., after a significant incident).
- Maintain a risk profile for use in disclosures, including the exposure determination process and result, recent trends of enterprise improvement, peer trends, and contingency strategies to inform periodic and incident-driven disclosures.

Information gained and adjustments to priority, risk appetite, and budget are then provided through the next iteration of Step 1.

While the steps above describe the aggregation of risk registers and risk profiles at the enterprise level, similar activities occur throughout the organization. System risk registers may be prioritized into system risk profiles, which may then be aggregated into risk registers at the next level, such as department or organization. As these are prioritized, they become organizational risk profiles that support an aggregated portfolio risk register. OMB Circular A-123 requires that "agencies must complete their initial risk profiles in coordination with the agency Strategic Reviews," and "no less than annually, all agencies must prepare a complete risk profile and include required risk components and elements required by this guidance."

This process also enables discussion about cybersecurity risks in relevant terms for each target audience. Detailed operational discussions may occur in Steps 2 and 3, while more abstracted information may be used for executives and the board in Steps 1 and 4.

The steps discussed above generate risk reports. From NISTIR 8170 [4], regarding federal agencies:

"Reports often need to be distributed to a variety of audiences, including business process personnel who manage risk as part of their daily responsibilities; senior executives who approve and are responsible for agency operations and investment strategies based on risk, other internal units; and external organizations. This means that reports need to be clear, understandable, and vary significantly in both transparency and detail, depending on the recipient and report requirement. Furthermore, reporting timelines need to match expectations of the receiving parties in order to minimize the time between the measurement of risk and delivery of the report. A standardized reporting format can assist agencies in meeting multiple cybersecurity reporting needs."

4.4 Conclusion

Cybersecurity events can have consequences that compromise the integrity of financial statements (e.g., income statement, balance sheet, cash flow), assurance statements,[29] and risk narratives in quarterly reports. They certainly impact enterprise objectives established or influenced by different stakeholders (e.g., Congress, regulators, taxpayers, shareholders, clients,

[29] Risk assessments directly inform annual assurance statements regarding the effectiveness of management controls (including system controls), both in public and private sector. This is because they apply the same best practices and standards for risk management and internal controls. Per OMB Circular A-123 for government, assurance statements are directly informed by risk analysis in a broad array of areas, including financial and non-financial.

public, partners). Board and Enterprise risk officers' recognition and attention to these and other enterprise vulnerabilities may become a demonstration of "duty of care" as the last line of protection for legal and regulatory risk.

Through the mission-based portfolio approach outlined in this section, senior executives can ensure that individual cybersecurity risks at the system level may be collected and analyzed for their alignment with and impact on enterprise strategic objectives. This collective understanding helps enterprise leaders stay aware of and assess substantial cybersecurity risk changes, review risk and performance results, and continually pursue improvement within the broader ERM to help the organization achieve its stated mission.

1877 # References

[1] Office of Management and Budget (2019) Preparation, Submission, and Execution of the Budget. (The White House, Washington, DC), OMB Circular No. A-11, December 18, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[2] Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC) (2016) Playbook: Enterprise Risk Management for the U.S. Federal Government. Available at https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf

[3] Office of Management and Budget (2016) OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. (The White House, Washington, DC), OMB Memorandum M-16-17, July 15, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[4] Marron J, Pillitteri V, Boyens J, Quinn S, Witte G, Feldman L (2020) Approaches for Federal Agencies to Use the Cybersecurity Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8170. https://doi.org/10.6028/NIST.IR.8170

[5] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[6] International Organization for Standardization (ISO) (2009) Risk management – Vocabulary. ISO Guide 73:2009. https://www.iso.org/standard/44651.html

[7] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[8] Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2017) Enterprise Risk Management—Integrating with Strategy and Performance, Executive Summary. Available at https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[9] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[10] International Organization for Standardization (ISO) (2018) Risk management—Guidelines. ISO 31000:2018. https://www.iso.org/standard/65694.html

[11] U.S. Government Accountability Office (GAO) (2014) Standards for Internal Control in the Federal Government. https://www.gao.gov/assets/670/665712.pdf

[12] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[13] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[14] Forum of Incident Response and Security Teams (FIRST) (2019) Common Vulnerability Scoring System version 3.1 Specification Document, Revision 1. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

[15] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[16] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/privacy-framework/privacy-framework

[17] Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2017) Internal Control—Integrated Framework, Executive Summary. Available at https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

[18] Software Engineering Institute (2007) Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. (Software Engineering Institute, Pittsburgh, PA), Technical Report CMU/SEI-2007-TR-012. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[19] The MITRE Corporation (2019) ATT&CK. Available at https://attack.mitre.org

[20] U.S. Securities and Exchange Commission (SEC) (2018) Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf

[21] International Electrotechnical Commission (IEC) (2019) Risk management – Risk assessment techniques. IEC 31010:2019. https://www.iso.org/standard/72140.html

[22] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

1878

Appendix A—Acronyms and Abbreviations

Selected acronyms and abbreviations used in this paper are defined below.

AFR	Agency Financial Report
BIA	Business Impact Analysis
BYOD	Bring-Your-Own-Device
CapEx	Capital Expenditures
CBA	Cost/Benefit Analysis
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CFOC	Chief Financial Officers Council
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations
COSO	Committee of Sponsoring Organizations
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSAM	Cyber Security Assessment and Management
C-SCRM	Cyber Supply Chain Risk Management
DHS	Department of Homeland Security
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
ERM	Enterprise Risk Management
ERSC	Enterprise Risk Steering Committee
FIRST	Forum of Incident Response and Security Teams
FOIA	Freedom of Information Act
GAO	U.S. Government Accountability Office
GRC	Governance/Risk/Compliance
HVA	High-Value Asset
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISCM	Information Security Continuous Monitoring

1910	ISO	International Organization for Standardization
1911	IT	Information Technology
1912	ITL	Information Technology Laboratory
1913	KPI	Key Performance Indicator
1914	KRI	Key Risk Indicator
1915	NCCoE	National Cybersecurity Center of Excellence
1916	NFC	National Finance Center
1917	NIST	National Institute of Standards and Technology
1918 1919	NISTIR	National Institute of Standards and Technology Interagency or Internal Report
1920	NOAA	National Oceanic and Atmospheric Administration
1921	OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
1922	OLIR	Online Informative References
1923	OMB	Office of Management and Budget
1924	OpEx	Operating Expenses
1925	OT	Operational Technology
1926	PIC	Performance Improvement Council
1927	POA&M	Plan of Action and Milestones
1928	RAR	Risk Assessment Report
1929	RMC	Risk Management Council or Committee
1930	RMF	Risk Management Framework
1931	SAORM	Senior Accountable Official for Risk Management
1932	SEC	U.S. Securities and Exchange Commission
1933	SEI	Software Engineering Institute
1934	SP	Special Publication
1935	SWOT	Strengths, Weaknesses, Opportunities, Threats
1936	US-CERT	United States Computer Emergency Readiness Team

Appendix B—Glossary

Actual Residual Risk	"The risk remaining after management has taken action to alter its severity." [8]
Aggregation	The consolidation of similar or related information.
Assets	"The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes." [15]
Context	The environment in which the enterprise operates and is influenced by the risks involved.
Cybersecurity Risk	An effect of uncertainty on or within a digital context. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (Definition based on ISO Guide 73 [6] and NIST SP 800-60 Vol. 1 Rev. 1 [7])
Enterprise	A top-level organization with unique risk management responsibilities based on its position in the hierarchy and the roles and responsibilities of its officers.
Enterprise Risk	The effect of uncertainty on enterprise mission and objectives.
Enterprise Risk Management	"An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos." [1] The "culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value." [8]
Enterprise Risk Register	A risk register at the enterprise level that contains normalized and aggregated inputs from subordinate organizations' risk registers and profiles.
Exposure	The combination of likelihood and impact levels for a risk.
Information System	"A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." [from OMB A-130]

Inherent Risk	"The risk to an entity in the absence of any direct or focused actions by management to alter its severity." [8]
Internal Control	An overarching mechanism that an enterprise uses to achieve and monitor enterprise objectives.
Normalization	The conversion of information into consistent representations and categorizations.
Opportunity	A condition that may result in a beneficial outcome.
Organization	An entity of any size, complexity, or positioning within a larger organizational structure (e.g., a federal agency or a company). [5]
Plan of Action and Milestones	A document for a system that "identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones." [13]
Qualitative Risk Analysis	A method for risk analysis that is based on the assignment of a descriptor such as low, medium, or high.
Quantitative Risk Analysis	A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain.
Residual Risk	Risk that remains after risk responses have been documented and performed.
Risk	"The effect of uncertainty on objectives." [1]
Risk Appetite	"The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value." [8] "The broad-based amount an enterprise is willing to accept in pursuit of its mission/vision." [3]
Risk Profile	"A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks." [3]
Risk Register	"A repository of risk information including the data understood about risks over time." [1]

Risk Reserve	A types of management reserve where funding or labor hours are set aside and employed if a risk is triggered to ensure the opportunity is realized or threat is avoided.
Risk Response	A way to keep risk within tolerable levels. Negative risks can be accepted, transferred, mitigated, or avoided. Positive risks can be realized, shared, enhanced, or accepted.
Risk Tolerance	The organization's or stakeholder's readiness to bear the remaining risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be influenced by legal or regulatory requirements. [6]
Security Control	"Safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information."
Semi-Qualitative Risk Analysis	A method for risk analysis with qualitative categories assigned numeric values to allow for the calculation of numeric results.
System	"A discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." [5]
Target Residual Risk	"The amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk." [8]
Threat	Any circumstance or event with the potential to adversely impact organizational operations (a negative risk).
Threat Actor	The instigators of risks with the capability to do harm.
Threat Source	A malicious person with harmful intent or an unintended or unavoidable situation (such as a natural disaster, technical failure, or human error) that may trigger a vulnerability.
Vulnerability	A condition that enables a threat event to occur.

1938

Appendix C—Federal Government Sources for Identifying Risks

This appendix lists Federal Government sources for identifying risks, as defined on page 28 of *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2]. Note that these are intended to supplement risk management programs and do not by themselves constitute the foundation of a risk management program.

- Agency Reports and Self-Assessments
  - Previous year Federal Managers and Financial Integrity Act reports and A-123, Appendix A self-assessments and related assurance statements. Specifically, this may include:
    - Entity-level control interviews and evidence documentation
    - Assessment of agency processes and thousands of documented controls
    - Documentation of control deficiencies, including the level of significance of those deficiencies (i.e., simple, significant, or material weakness)
    - Corrective actions associated with the deficiencies and tracked to either remediation or risk acceptance
  - Financial Management Risks documented in the agency's Annual Report
  - Project management risks documented in the agency's investment and project management processes
  - Anything raised during Strategic Objectives Annual Review, quarterly performance reviews, RMC, etc.
- Inspector General (IG) and Government Accountability Office (GAO)
  - IG Management Challenges documented annually in the agency's AFR
  - IG audits and the outstanding corrective actions associated with those audits
  - GAO audits and the outstanding corrective actions associated with those audits
- Congress
  - Issues and risks identified during Congressional Hearings and Questions for the Record
- Media
  - Issues and risks identified in the news media

Note: RMC stands for Risk Management Council or Committee, and AFR stands for Agency Financial Report.